VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

Metódy merania výkonnostných a kvalitatívnych parametrov dátových sietí

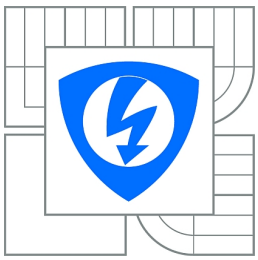
Methods for measurement of data network performance and quality parameters

DIPLOMOVÁ PRÁCA
MASTER´S THESIS

AUTOR PRÁCE — Bc. Luboš Sukup
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Vít Novotný, Ph.D.
SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Luboš Sukup	***ID:***	83209
Ročník:	2	***Akademický rok:***	2011/2012

NÁZEV TÉMATU:

Metody měření výkonnostních a kvalitativních parametrů datových sítí

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte různé typy služeb z hlediska jejich požadavků na prostředky komunikačního řetězce (koncových zařízení, spojů, přepojovacích uzlů a bezpečnostních prvků). Posuďte vlivy jednotlivých typů komponentů datových sítí založených na protokolové sadě TCP/IP na výkonnostní a kvalitativní parametry služeb a prozkoumejte možnosti jejich měření. V závislosti na dostupném vybavení vybrané metody prakticky ověřte a navrhněte laboratorní úlohu včetně návodu.

DOPORUČENÁ LITERATURA:

[1] SZIGETI, T., HATTINGH, CH. End-to-End QoS Network Design. Cisco Press, ISBN 1-58705-176-1, USA, 2004

[2] BEURAN, R., IVANOVICI, M., DOBINSON, B. Network Quality of Service Measurement System for Application Requirements Evaluation. Proceedings of the 2003 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2003), July 20-24, 2003, Montreal, Canada, ISBN: 1-56555-269-5, pp.380-387, 2003

Termín zadání:	6.2.2012	***Termín odevzdání:***	24.5.2012

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.
Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

Metódy merania výkonnostných a kvalitatívnych parametrov dátových sietí

Methods for measurement of data network performance and quality parameters

DIPLOMOVÁ PRÁCA
MASTER´S THESIS

AUTOR PRÁCE — Bc. Luboš Sukup
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Vít Novotný, Ph.D.
SUPERVISOR

BRNO 2012

ABSTRAKT

Diplomová práca obsahuje vypracovanie problematiky merania kvalitatívnych a výkonnostných parametrov v dátových sieťach. Sú tu popísané hlavné technológie ako ovplyvňujú kvalitatívne a výkonnostné parametre a vplyv na týchto parametrov na hlasové, video a dátové služby. Ďalej sú vymenované niektoré metódy merania parametrov dátovej siete. V praktickej časti je vybraná jedna metóda merania parametrov siete a vlastnosti tejto metódy sú demonštrované na názorných príkladoch.

KĽÚČOVÉ SLOVÁ

kvalitatívne parametre, výkonnostné parametre, oneskorenie, latencia, jitter, dátová sieť, TCP, IP, TCP/IP, chybovosť, meranie, kvalita, QoS, QoE, RTT, priepustnosť, Netflow, Syslog, Wireshark, riadiaca sieť,

ABSTRACT

Master thesis involves the development of quality measurement issues and performance parameters in data networks. It describes the main technologies as they affect the quality and performance parameters and the effect of these parameters for voice, video and data services. Next are listed some methods for measuring parameters of the data network.
In the practical part is selected one method of measuring network parameters and properties of this method are demonstrated by illustrative examples.

KEYWORDS

quality parameters, performance parameters, delay, latency, jitter, data network, TCP, IP, TCP / IP error, measurement, quality, QoS, QoE, troughtput, Netflow, Syslog, Wireshark, management network,

SUKUP, L. *Metódy merania výkonnostných a kvalitatývnych parametrov dátových sietí* . Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2012. 10 s., 4 s. příloh. Diplomová práca. Vedoucí práce: doc. ing. Vít Novotný, Ph.D.

PREHLÁSENIE

Prehlasujem, že svoju diplomovú prácu na téma *Metódy merania výkonnostných a kvalitatývnych parametrov dátových sietí* som vypracoval samostatne pod vedením vedúceho diplomovej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, najmä nezasiahol nedovoleným spôsobom do cudzích autorských práv osobných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúceho zákona č. 121/2000 Sb., o práve autorskom, o právach súvisiacimi s právom autorským a zmene niektorých zákonov(autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka č. 40/2009 Sb.

V Brne dňa ....

(podpis autora)

POĎAKAVANIE

Ďakujem vedúcemu diplomovej práce doc. ing. Vítu Novotnému, Ph.D. za účinnú metodickú, pedagogickú a odbornú pomoc a ďalšie cenné rady pri spracovávaní mojej diplomovej práce.

V Brne dňa ....

(podpis autora)

Obsah

1 Úvod

V dnešnej dobe, keď sa v telekomunikačnom prostredí vo veľkom nasadzujú riešenia konvergovaných sietí zlučujúcich dáta, hlas, video do jedného logického paketového celku, je nutné sa zamyslieť nad kvalitatívnymi a výkonnostnými požiadavkami týchto jednotlivých zložiek. Z týchto dôvodov je nutné zabezpečiť požadovanú kvalitu služieb v cez celú trasu od odosielateľa ku príjemcovi. V prípade vzniku situácie na sieti, ktorá napríklad spôsobí rapídne zníženie prenosovej rýchlosti na jednom sieťovom prvku, toto zníženie rýchlosti sa prejaví na zostatku trasy smerujúcej k príjemcovi aj keď zvyšok trasy je v poriadku.

Cieľom tejto práce je vymenovať metódy akými je možne merať parametre dátových sietí. Úlohou práce je vymenovať tieto parametre a ako vplývajú na služby, ktoré využívajú užívatelia sietí. Tieto služby sú hlavne prenos hlasu, prenos videa a prenos bližšie neurčených dát. Spolu so službami budú vymenované potrebné požiadavky týchto služieb na dátové siete. V ďalšej časti budú popísané metódy merania a diagnostiky sietí vlastnosti jednotlivých metód. V praktickej časti bude vybraná jedna metóda merania parametrov sietí a a budú ňou zmerané požadované parametre.

2 Služby v telekomunikácii

Definovať telekomunikačnú službu môžeme takto: Telekomunikačnou službou je chápaný prenos informácií v podobe signálov, nesúce zvukové, textové, či obrazové vyjadrenie, telekomunikačným systémom. Tieto služby môžeme kategorizovať podľa niekoľkých hľadísk napríklad: rozdelenie podľa spracovania informácie, podľa vývoja potrieb užívateľa, podľa súčasne komunikujúcich užívateľov atď.
Pre využiteľnosť pre túto prácu sa zvolilo rozdelenie podľa dostupnosti služieb a to je rozdelené na:

- bezdrôtové
  - služby GSM štandardov
  - služby bezdrôtových paketových sietí (Wifi)
- pevné
  - digitálne integrované služby ISDN
  - služby asynchrónnych sietí ATM
  - služby poskytované v sieťach LAN
  - služby internetového charakteru

Kvalita služieb je výrazne závislá od použitého média, ktoré je použité na prenos dát. Tak aj metódy na zvýšenie kvality služieb poskytovaných užívateľom sa líšia pri využití vzduchu alebo metalického a optického vedenia.

3 Služby bezdrôtových sietí

Bezdrôtové dátové siete sú úplne odkázané na rádiové prenosové prostredie. Z fyzikálneho princípu šírenia rádiových vĺn v porovnaní s pevným vedením má rádiové prenosové prostredie takmer samé nevýhody. Nevýhody, ktoré tieto dátové siete majú najviac problémov spôsobuje mnohocestné šírenie signálu, ktoré vyvolá:

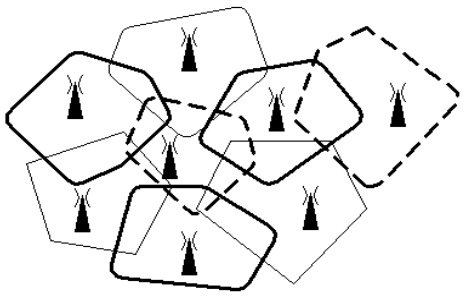
- značnú nestabilitu prenosových charakteristík (amplitúdovo-frekvenčná charakteristika, skupinové oneskorenie, útlm) prenosového kanálu
- selektívne zoslabenie nebo úplné vytratenie časti spektra signálu, čo práve pri prenose dát vyššími prenosovými rýchlosťami spôsobuje vážne komplikácie
- veľmi nerovnomerné rozloženie intenzity elektromagnetického poľa, spôsobené skladaním priamej a odrazenej elektromagnetické vlny. Takto deformované elektromagnetické pole sa vždy vyskytuje vnútri budov a v husto zastavaných miestach, kde použitie rádiových sietí na prenos dát je najviac využiteľné. A toto nerovnomerné rozloženie intenzity elektromagnetického poľa spôsobuje problémy v mobilnom použití koncového zariadenia. Napríklad pri jeho použití v dopravnom prostriedku, kedy intenzita poľa veľmi rýchlo kolíše čím vzniká veľmi rýchli únik o frekvencii rádovo desiatok Hz (tzv. Rayleighov únik) a k tomu aj posuv nosnej frekvencie vplyvom Dopplerova efektu
- prevažne veľmi nízku úroveň prijímaného vysokofrekvenčného signálu a tým nebezpečenstvo príjmu rôznych rušení, alebo nežiaduceho vyžarovania od iných rádiových prostriedkov
- pomerne ľahkú možnosť nežiaduceho dopočutia prenášaných

Jedinou výhodou rádiového prenosového prostredia je že prípojným bodom koncového zariadenia je celá oblasť pokrytá vysokofrekvenčným signálom o vyššej ako je prahová intenzita elektromagnetického poľa a dostatočnej kvalite signálu

O hodne jednoduchšia je situácia pri rádiovom spojení medzi dvoma pevnými bodmi , kedy je možné použitím smerových antén a ich vhodným umiestnením vyššie uvedené problémy potlačiť.

3.1 Služby GSM štandardov

GSM teda Global system for mobile communications vie prenášať nie len hlas ale aj textové správy SMS a dáta. Prenos dát cez GSM sa začal implementovať od roku 1995. Systém využíva plne duplexný prenos s frekvenčným delením FDD. Systém GSM je tvorený bunkami o priemere veľkosti 1-3 km. Obyčajne v hustejšie obývaných oblastiach je tento priemer nižší asi 500m a naopak v v riedko osídlených oblastiach tento priemer bunky môže byť aj 30 km.

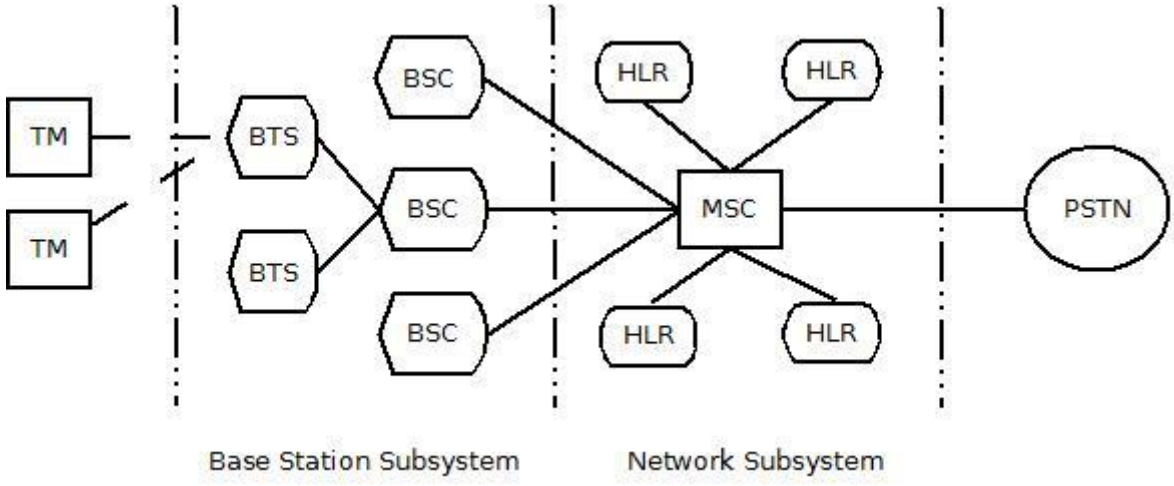


Obr.1 príklad buniek v GSM

Architektúra GSM

GSM sieť môžeme rozdeliť do troch subsystémov:

- **subsystém základňových staníc – BSS** (*Base Station Subsystem*)
- **sieťový a spínací subsystém – NSS** (*Network and Switching Subsystem*)
- **operační a podporný subsystém - OSS** (*Operation and Support Subsystem*



Obr.2 Architektúra GSM

Subsystém základňových staníc BSS je zložený z určitého počtu základňových staníc BTS (Base Transciever Station) zaisťujú komunikáciu medzi mobilnými stanicami (obyčajne to býva mobilný telefón).
BSC (Base Station Controler) stará sa o chod rádiového rozhrania prideľovania a uvoľňovania rádiových kanálov, komunikuje s ústredňou a a stará sa o handover (predávania hovorov medzi buňkami). BSC ovláda viacero BTS.

Sieťový a spínací subsystém NSS (Network switching subsystem) prakticky vykonáva prácu ako u pevnej linky ústredňa. Riadi komunikáciu medzi mobilnými účastníkmi siete GSM a komunikáciu s ďalšími externými sieťami. Z jednej strany je spojený so všetkými dostupnými BTS a z druhej strany je pripojený na všetky externé siete.
Podsystémy NSS sú:

- **mobilná spínacia ústredňa MSC** (mobile services switching center). Slúži ako klasická ústredňa v pevnej sieti napríklad prepínanie hovorov.

- **domovský lokalizační register HLR** (home location register) Jedná sa o databázu, kde sú údaje o všetkých registrovaných účastníkoch.
- **návštevnícky lokalizační register VLR** (visitor location register). Tu sa uchovávajú aktuálné informácie o mobilných účastníkoch pohybujúcich sa v oblasti.
- **autentizačné centrum AUC** (authentication center). Overenie identity účastníka
- **register mobilných staníc EIR** (equipment identity register). Táto databáza obsahuje identifikačné čísla (IMEI) mobilných telefónov.
- **SMS centrum SMSC** - centrum kam prichádzajú všetky SMS.

3.1.1 Dátové prenosy v sieťach GSM

HSCSD (High Speed Circuit Switched Data)

GSM sieť bola pôvodne navrhnutá ako sieť spínacích okruhov typická pre prenos hlasu. Dátové služby boli do štandardu implementované aktualizáciou nazvanej Phase 2. Základná prenosová rýchlosť bola 9,8 kbit.s^{-1}. Táto základná dátová rýchlosť nebola dostačujúca a tak bola navrhnutá inovácia HSCSD (High Speed Circuit Switched Data). Táto implementácia umožňovala prideľovanie viacero timeslotov pre jedného užívateľa. Tak sa maximálna prenosová rýchlosť zvýšila na 14,4 kbit.s^{-1}. Keďže je HSCSD postavené na prideľovaní timeslotov jednému užívateľovi tak sa týmto spôsobom znižoval celkový počet účastníkov. Výhoda tohto navýšenia prenosovej rýchlosti bola, že sa stávajúce hardwarové vybavenie nemuselo meniť.

GPRS (General Packet Radio Service)

Keďže spínacie okruhy nie je vhodná na prenos dát spoločnosť Ericsson vyvinula službu, ktorá umožňuje súbežne využívať hlasové služby a aj paketový prenos. Zmenou spôsobu komunikácie na paketový prenos je možné meniť dynamicky prenosovú rýchlosť pre jedného užívateľa.

Pre kódovanie signálu pre GPRS sú dané štyri rôzne kódovacie schémy. CS (coding scheme) 1 – 4. Odolnosť voči chybám je najvyššia u CS1 a klesá k CS4. Kde CS4nemá žiadnu ochranu voči chybám a využíva sa v miestach kde je veľmi kvalitný signál. U CS4 je stanovená teoretická prenosová rýchlosť na 171,1 kbit.s^{-1} a užívateľská rýchlosť sa pohybuje okolo 133,6 kbit.s^{-1}.

EDGE (Enhanced Data Rates for GPRS Evolution)

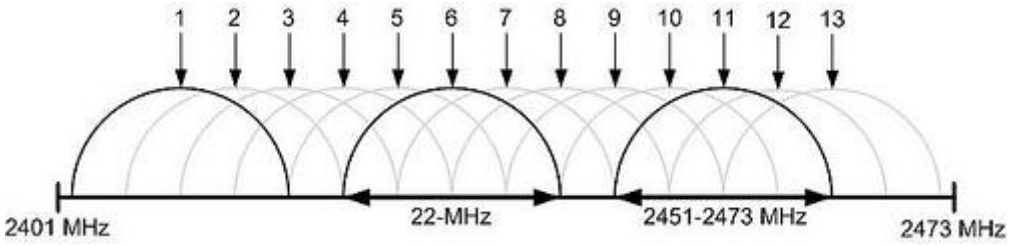
Ďalším stupňom pri poskytovaní vyšších rýchlostí pri mobilnej dátovej komunikácii je EDGE. Zmena oproti GPRS je zmena modulácie, ktorá umožňuje pri rovnako širokom frekvenčnom kanále vyššiu prenosovú rýchlosť.
Služby GSM siete sú: uskutočnenie hovoru, zobrazenie čísla volajúceho, blokovanie hovorov, čakajúci hovor atď.

3.2 Dátové prenosy v paketových bezdrôtových sietí WIFI

Bezdrôtové dátové siete majú asi najväčšie zastúpenie a najväčšie povedomie verejnosti ako bezdrôtová sieť. WIFI vychádza zo štandardu 802.11. Tento štandard bol navrhnutý na bezlicenčnú frekvenciu v rozsahu 2,4-2,485 GHz. Pôvodne bolo WIFI založené na troch technológiách. CDMA (Code Division Multiple Access) a na priame rozprestieranie DSSS (Direct Sequence Spread Spectrum). Tretia technológia je infračervený prenos. Pôvodná maximálna prenosová rýchlosť bola 2Mb.s^{-1}. Ďalšie rozšírenia štandardu sú 802.11b kde prenosová rýchlosť je 11 Mb.s^{-1}, 802.11a s maximálnou prenosovou rýchlosťou 54 Mb.s^{-1} . Zariadenia WIFI môžu pracovať v niekoľkých režimoch sieťovej prevádzky a to:

- Access point
- Bridge
- Router
- Ad-Hoc

Fyzická vrstva ktorá je najnižšie položenou vrstvou má na starosti samotné vysielanie a príjem dát bezdrôtovým prostredím.
Frekvenčné pásmo 2,4 – 2,485 GHz je rozdelené na 13 kanálov o šírke 22 MHz kde sa neprekrývajú len 3 kanály a to prvý, šiesty a jedenásty kanál.



Obr.3 frekvenčné pásma Wifi

3.2.1Kvalita a rýchlosť prenosu dát pri WIFI

Rýchlosť a kvalita prenášaných dát je daná jeho moduláciou. Pri zmene modulácie dochádza aj ku zmene rýchlosti a citlivosti. Modulácie, ktoré sú použité pri bezdrôtovom prenose sú:
- DSSS (Direct Sequence Spread Spectrum) priame rozprestieranie pomocou pseudonáhodnej postupnosti sa využíva u 802.11b
- FHSS (Frequency Hopping Spread Spectrum) rozprestieranie pomocou frekvenčných skokov sa využíva prevažne u bluetooth.
- OFDM (Orthogonal Frequency Division Modulation) sa využíva u 802.11 a,g.

Prenosová rýchlosť je vždy uvedená ako bitová rýchlosť na fyzickej vrstve pre obidva smery vrátane riadiacich informácií. Pri náraste rušenia v prenosovom prostredí dochádza k opakovanom prenose paketu tzv. retransmisson, ktoré je definované

fyzickou vrstvou a nemá priamu súvislosť s opakovaním prenosu paketu protokolu TCP/IP. Toto sa prejaví značným znížením užívateľskej rýchlosti prenesených dát a výrazne zvyšuje latency prenosu. To výrazne sťažuje využitie služby VoIP.

Siete Wifi využívajú na prístup ku zdieľanému médiu techniku CSMA-CA (Carier Sence Multiple Access Colision Avoidance). Ak dôjde pri vysielaní stanici A k detekcii prevádzky v prenosovom kanále, vysielacia stanica na náhodne dlhú dobu čaká na ďalší pokus o detekciu aktivity v prenosovom kanále. Ak je kanál voľný, stanica A začne vysielať. Pri prevádzke v kanále dôjde k ďalšiemu čakaniu pred ďalším pokusom o vysielanie.

3.2.2 Ochrana dát proti chybám prenosu a prostriedky na ich odstránenie

Ochrana proti chybám má u mobilných sieti zásadný význam. Pri prenose hlasového signálu nebol kladený taký dôraz na kvalitu signálu. U hlasového signálu je akceptovaný určitý pokles kvality kde človek má schopnosť pri krátkom narušení integrity hlasového signálu domyslieť si chýbajúcu časť hovoru. Ale nástupom mobilných sietí podporujúci dátový prenos nároky na kvalitu a integritu dátového toku výrazne vzrástlo.

Interleaving a scrambling

Interleaving, alebo prekladanie dát, je založené na tom, že sa dáta ukladajú do vyrovnávacej pamäte v tvare štvorcovej matice napríklad po riadkoch a čítajú sa po stĺpcoch. Ak dôjde pri prenose ku strate skupiny susedných bitov, tak sa po spätnom ukladaní do matice v prijímači tento zhluk chýb rozprestrie do krátkych chýb a tieto chyby sa dajú opraviť samo opravným kódom .

Scrasmbling je založený na vynásobení (logický súčin) bloku dát pseudonáhodnou sekvenciou rovnakej dĺžky. Týmto vynásobením získa dátový signál výhodnejšie vlastnosti na prenos. Týmto sa odstráni zo signálu dlhé sekvencie jednotiek ale lebo núl.

Samo opravné kódy

Dôležitým opatrením na zníženie chybovosti prenosu je vhodné kódovanie signálu na prenos rádiovým kanálom. Podstatou je systematické pripojovanie redundancie tak, aby dekodér preskúšaním správnosti prijatého kódového slova mohol detekovať chyby (detekčné kódy) alebo - pri dostatočne vysokej redundancii - rekonštrukciou kódového slova chyby odstrániť (korekčné kódy).
Korekčných kódov je viacero druhov. Reed - Solomonove kódy RS (N,K) opravujú zhluky (N-K)/2 chýb a indikujú zhluky (N-K) chýb. Napríklad kód RS (255,239) je schopný opraviť zhluk až 8 chyb a indikovať zhluk až 16 chýb.
Fireove kódy sú tak isto ako Reed – Solomonove cyklické blokové kódy.

Prevádzka ARQ

Spočíva v tom, že sa tok dát rozdelí na bloky, ktoré sa zabezpečia napríklad kontrolným súčtom a na prijímacej strane sa kontroluje správnosť prijatého bloku. Pokiaľ blok nie je prijatý bez chyby, prenos bloku sa opakuje. Existuje niekoľko typov ARQ podľa toho, či a akým spôsobom sa prenose používa tiež korekcia chýb.

Modulácia OFDM

U prenosov dát vyššími rýchlosťami (rádovo stovky kbit/s až jednotiek Mbit/s) je možné čeliť účinkom viaccestného šírenia vysokofrekvenčného signálu rozdelením toku dát na viacej vysokofrekvenčných subnosných frekvencií, ktoré sa vysielajú súčasne a ktoré sú modulované dátami s pomerne nízkou prenosovou rýchlosťou. Väčšina odrazených signálov má veľmi malé časové oneskorenie, rádovo desiatky nanosekúnd až jednotky mikrosekúnd. Pri prenose dát vysokými rýchlosťami je časová dĺžka jedného bitu porovnateľná s časovým oneskorením odrazeného signálu, čo spôsobuje deštrukciu dát. Pri rozdelení toku dát na jednotlivé subnosnej nedochádza k deformácii tvaru dát, pretože 1 bit dátového signálu ma v porovnaní s časovým oneskorení odrazeného signálu podstatne dlhšiu dobu trvania. Tento modulačný systém je používaný pri prenose vysokofrekvenčnom signálu pozemnom digitálnom rozhlase a pozemnej digitálnej televízie a je veľmi odolný proti viaccestnému šíreniu a je vhodný pre mobilný príjem.

Zaistenie dostatočne vysokej intenzity elektromagnetického poľa pre spojení

Takejto intenzity je možné dosiahnuť len vyššou intenzitou elektromagnetického poľa pri dátovom prenose ako je pri prenose hlasu. Druhá možnosť je výstavba dostatočného počtu BSS staníc a pri poklese intenzity presmerovať komunikáciu na BSS stanicu kde má signál vyššiu intenzitu. Toto je možné len pri dostatočne rýchlom presmerovaní spojenia rádovo v jednotkách milisekúnd.

4 Služby pevných dátových sietí

Pevné siete na prenos dát používajú prenosové prostredie prevažne vo forme metalických alebo optických vedení. Tieto prenosové prostredia oproti bezdrôtovým dátovým sieťam majú viacero výhod. K najväčším výhodám patria:

- stabilita prenosových charakteristík a útlmu prenosového kanála
- dosiahnuteľná vysoká rýchlosť prenosu (rádovo až niekoľko Gbit/s), čo umožňuje budovanie tzv. informačných diaľnic na základe technológie ATM,SDH, Frame releay
- šírenie signálu je lokalizované len na danú prenosovú cestu, mimo nej nie je signál dostupný

Tak ako mobilné siete aj pevné siete je možné rozdeliť lokálne poprípade metropolitné siete a chrbtové siete. Takéto delenie je rozdelené podľa technológie akú tá daná sieť podporuje. Sú to prepojovanie okruhov a prepojovanie paketov.

Medzi siete prepájajúce okruhy patria ATM alebo ISDN. Spojovo orientované siete sú charakteristické tým, že fungujú spojovo. Prenos môže byť buď prúdový alebo aj blokový charakter. Prenos má garantovanú kvalitu. Prenosové oneskorenie je veľmi malé, rozptyl prenosového oneskorenia je malý. Dáta nepoužívajú princíp store&forward. Funguje hlavne vo svete spojov. Hlavné zastúpenie má u telefónnej siete, ISDN.

Prepojovanie paketov môže byť spojové ale aj nespojové. Môže mať len blokový charakter. Prenos má charakter best effort, dáta sa po ceste ukladajú.

V tejto časti práce vymenovania a popísania služieb, ktoré v prevažnej väčšine pracujú na pevných dátových sieťach by bol zvolený iný spôsob triedenia. Pri zachovaní stávajúceho triedenia by malo byť vymenované akými médiami sú siete prepojené (metalické vedenie, optické vedenie). Miesto toho bolo vybrané delenie podľa veľkosti oblastí a podľa toho akú službu prevažne využíva.

Local Area Network

Lokálna sieť spája počítače a sieťové zariadenia v ohraničenej geografickej oblasti. Môže to byť škola, budovy škôl, kancelárska budova ect. Každý počítač a zariadenie sa v tejto sieti nazýva uzol. Stávajúce pevné siete LAN väčšinou bežia na technológii Ethernet.

Všetky prepojené zariadenia musia vedieť pracovať na tretej vrstve OSI modelu, lebo je potrebne aby dokázali komunikovať so zariadeniami v iných podsietí. .Stávajúce technológie ako Ethernet alebo iné LAN technológie odvodené z IEEE 802.3 pracujú obyčajne do 10 Gbit/s. Do budúcnosti je tendencia túto rýchlosť zvyšovať.

Metropolitan Area Network

Táto sieť pokrýva oblasť o veľkosti mesta a skladá sa z väčšieho počtu LAN sietí navzájom pospájaných hraničnými uzlami. Prepojenie sa deje pomocou optických vlákien ale ako prepojenie môže slúžiť aj nejaká bezdrôtová technológia.

Wide Area Network

Siete WAN sú využívané na prepojenie LAN sietí alebo iných typov sietí, takže užívatelia z jedného miesta môžu komunikovať s užívateľom a počítačom na inom mieste. Veľa WAN sietí je budovaná ako podnikové siete a sú súkromné. Siete WAN sa obyčajne budujú na prenajatých linkách. Častejšie sa siete WAN budujú na metódach prepojovania okruhov (circuit switching) alebo na prepojovaní paketov (packet switching). Sieťové služby používajú na prenos a adresovanie protokol TCP/IP. Poskytovatelia služieb pripojenia častejšie využívajú na prenos v sieťach WAN protokoly ATM a Frame Relay.

4.1 Model TCP/IP a vplyv na QoS

Drvivá užívateľov dátových sietí bez svojho vedomia využíva model TCP/IP so svojou protokolovou sadou. Protokolová sada TCP/IP vznikla v rámci výskumných prác zahájených ministerstvom obrany na pokusnej akademickej sieti ARPANET. Vzhľadom k tomu, že vývoj prebiehal ešte pred vznikom referenčného modelu OSI je model TCP/IP štvorvrstvový.

Model ISO/OSI	***Model TCP/IP***
7 Aplikačná vrstva	**4 Aplikačná vrstva**
6 Prezenčná vrstva	
5 Relačná vrstva	
4 Transportná vrstva	**3 Transportná vrstva**
3 Sieťová Vrstva	**2 Internet**
2 Linková Vrstva	**1 Sieťová vrstva**
1 Fyzická vrstva	

Tabuľka 1. Porovnanie modelov ISO/OSI a TCP/IP

4.2 Sieťová vrstva

Vrstva sieťového rozhrania zaisťuje fyzickú komunikáciu uzlov siete. Spája v sebe spojovú a fyzickú vrstvu Osi modelu. Naj používanejším protokolom je Ethernet. Ďalšie protokoly pracujúce na sieťovej vrstve sú napr.: WiMAX, ATM, Token ring.

4.2.1 Ethernet

Je prenosovou technológiou, ktorá zabezpečuje skutočný prenos dát a v RM ISO/OSI modelu pokrýva fyzickú a linkovú vrstvu. V rámci TCP/IP spadá do vrstvy sieťového rozhrania. Môže používať rôzne prenosové médiá. Chovanie má štatistické,

čo znamená, že nezaručuje právo vysielať len pravdepodobnosť. Klasický Ethernet používal zbernicovú topológiu teda zdieľané médium, kde v jednom okamžiku môže vysielať len jeden. Jednotlivé sanice pripojené k sieti sú identifikované svojimi hardwarovými adresami MAC. Sú to 48 bitové hodnoty kde prvých 24 bitov označuje spoločnosť, ktorá vyrobila sieťovú kartu a druhých 24 bitov značí unikátnu identifikáciu samotnej karty. Do budúcnosti sa pripravuje rozšíriť túto adresu na 64 bitov.

24 bitov	24 bitov
identifikátor OUI	**unikátna identifikácia NIC**

Obr.4 MAC adresa

Ak dostane stanica rámec s inou než svojou adresou zahodí ho. Na prístup k zdieľanému prenosovému médiu sa používa technológia CSMA/CD. Preto zdieľaný Ethernet nie je použiteľný tam, kde je potrebná odozva v určitom maximálnom čase. Po implementácii Ethernetu z koaxiálneho kábla na krútenú dvojlinku odpadá nutnosť využívať CSMA/CD lebo už na prichádzajúce a odchádzajúce dáta sú použité odlišné káble. Tento režim prevádzky sa nazýva full duplex. Odpadajú v ňom doby čakania spôsobené kolíziami a prenosová rýchlosť sa približuje maximálnej.

Typy Ethernetu.

- **10Base5** Pôvodní Ethernet na koaxiálnom kábli o rýchlosti 10 Mbit/s
- **10Base2** Ethernet na tenkom koaxiálnom kábli o rýchlosti 10 Mbit/s.
- **10Base-T** Ako prenosové médium sa používa krútená dvojlinka s rýchlosťou 10 Mbit/s. Využíva dva páry zo štyroch. Dnes už prekonaná sieť
- **10Base-F** Variant s optickými vláknami o rýchlosti 10 Mbit/s. Používa sa pre spojenie na väčšie vzdialenosti.
- **100Base-TX** Variant s prenosovou rýchlostí 100 Mbit/s, ktorej sa hovori **Fast Ethernet**, používa dva páry UTP nebo STP kabelu kategórie 5.
- **100Base-T2** Používá dva páry UTP kategórie 3, 4, 5.
- **100Base-T4** Používá čtyři páry UTP kategorie 3, 4, 5.
- **100Base-FX** Fast Ethernet používajúce dve optická vlákna.
- **1000Base-T** Ethernet s rychlostí 1000 Mbit/s, nazývaný **Gigabit Ethernet**. Využíva 4 páry UTP kabeláže kategórie 5e, je definovaný do vzdialenosti 100 metrov.
- **1000Base-CX** Gigabit Ethernet na bázi medeného vodiče na krátke vzdialenosti, učený pre prepojovanie skupín zariadení.
- **1000Base-SX** Gigabit Ethernet používajúci mnoho vidové optické vlákno. Je určený pre páteřní siete do vzdialenosti niekoľko sto metrov.
- **1000Base-LX** Gigabit Ethernet používajúci jedno vidové optické vlákno. Je určený pre väčšie vzdialenosti až niekoľko desiatok km.
- **10GBase-T** Ethernet s rýchlosťou 10 Gbit/s, nazývaný **Ten Gigabit Ethernet** (nebo také EFM - Ethernet on the first mile).
- **40GBASE** a **100GBASE** s rýchlosťou 40 a 100 Gbps by mal používať optické vlákna; medené káble do dĺžky aspoň 10 metrov.

V dôsledku navýšenia prenosovej rýchlosti sa Ethernet začína využívať aj u sietí WAN a MAN.

Pôvodne Ethernet pracoval na princípe best effort, ktorý nemé žiadne mechanizmy na riadenie toku. Toto rieši IEEE 802.3x.

4.3 Internetová vrstva

Internetová alebo podľa OSI modelu sieťová vrstva zaisťuje sieťové adresovanie a predávanie datagramov, datagramová služba. Táto vrstva je navrhnutá na čo najväčšiu prenosovú rýchlosť a to na úkor spoľahlivosti. Spoľahlivosť prenosu majú na starosti vyššie vrstvy modelu. Sieťová vrstva musí riešiť odlišnosťami jednotlivých sietí ako sú napríklad: odlišný charakter adries, rôzna prenosová rýchlosť, rôzna veľkosť paketov. Najznámejší protokol zo sieťovej vrstvy je protokol IP. Aktuálne beží IP protokol verzie 4 a postupne ho nahrádza protokol verzie 6. Ďalšie protokoly, ktoré operujú na internetovej vrstve sú: OSPF, IPsec, IGMP, ICMP, ICMPv6.

4.3.1 IPv4

IPv4 protokol patrí k najznámejšiemu a najvyužívanejšiemu protokolu internetovej vrstvy. IPv4 má za úlohu vytvoriť z jednotlivých sietí jednu homogénnu sieť. Presnejšie vytvoriť ilúziu jednej siete. Musí vyriešiť odlišnosti napríklad vo veľkosti paketov, rôzny charakter adries, inými prenosovými službami. (spojová, nespojová).

Dôležitou úlohou v rámci QoS a zaistenia požadovaných parametrov prenosu je smerovanie. Smerovanie má za úlohu vyhľadať cestu z jedného bodu cez rôzne prepojené siete k cieľovej stanici. Toto smerovanie zaisťujú zariadenia nazývané smerovače (routery), ktoré majú zadefinovanú, manuálne alebo automaticky, smerovaciu tabuľku. Podľa tejto smerovacej tabuľky sú pakety predávané ďalej cez iné smerovače až k cieľu.

4.4 Transportná vrstva

Transportná vrstva je označovaná ako TCP vrstva. Keďže najvyužívanejší protokol internetovej vrstvy IP protokol pracuje na princípe best effort tak kvalitu a spoľahlivosť, zamedzenie strácaniu dát, riadenie toku dát zaručuje práve transportná vrstva. Keďže ale existujú aj aplikácie, ktorých hlavným kritériom je rýchlosť a prípadnú stratu alebo chybovosť dát dokážu akceptovať na transportnej vrstve pracujú dva protokoly. TCP a UDP.

Jednotlivé aplikácie si majú možnosť vybrať, či je pre nich výhodnejšie používať na úrovni transportnej vrstvy nespoľahlivé ale výkonnejšie služby poskytované protokolom UDP alebo naopak použiť pomalšie ale zato spoľahlivejšie služby protokolom TCP.

4.5 Aplikačná vrstva

Aplikačná vrstva TCP/IP modelu nahrádza tri vrstvy OSI modelu a to relačnú prezenčnú a aplikačnú vrstvu. Jej entitami sú jednotlivé aplikačné programy, ktoré priamo komunikujú s transportnou vrstvou. Prípadné relačné alebo prezenčné služby si musí aplikácia realizovať sama. Aplikačné protokoly sú: DHCP, telnet, HTTP , FTP, IMAP, rôzne poštové protokoly ...

5 Kvalita služieb QoS a kvalita vnímania QoE

Meranie kvality dátového prenosu z väčšej časti závisí na koncovom užívateľovi. Akú službu užívateľ používa, aké sú nároky užívateľa. Toto sú najdôležitejšie faktory, ktoré odrážajú stav kvality dátového prenosu.

Pri zisťovaní a nastavovaní optimálnych parametrov na prenos dát sa vychádza z dvoch hľadísk. Jedným je kvalita služby známa ako Quality of Service (Qos) a kvality vnímania Quality of Experience (QoE).

QoS a jej parametre môžeme chápať ako objektívne hodnoty, ktoré zahŕňajú požiadavky na všetky aspekty spojenia, čo sú oneskorenie, strata dát, prenosová rýchlosť, priepustnosť, využitie siete, chybovosť a tak ďalej. Nazbierané hodnoty sa porovnajú s tabuľkovými hodnotami, ktoré sú všeobecne akceptované.

Oproti tomu kvalita vnímania a jej hodnoty sa môžu zhrnúť pod jeden názov ako subjektívny názor užívateľa. Je to vlastne celková spokojnosť s poskytovanými službami. Napríklad, bežní užívatelia očakávajú telefónny hovor cez IP sieť na rovnakej kvalite ako boli v minulosti zvyknutí. Ale napríklad pri mobilnej komunikácii alebo pri hovore cez mikrofón prepojený cez osobný počítač sú ochotní akceptovať určité zhoršenie kvality závislé od ich osobných skúseností, aj keď všetka prevádzka je uskutočňovaná cez jenu sieť. Tu je vidno, že subjektívne meranie parametrov silno závisí od každého užívateľa.

Hodnoty QoE sú dôležité najmä pre poskytovateľov pripojenia, keďže ich hlavným cieľom je zisk a ten sa dosiahne spokojnosťou zákazníka.

Trendom dnešnej doby je tzv. multiservice sieť, ktorá je schopná prenášať všetky typy komunikácie - hlas, dáta a video pomocou paketovej architektúry. Požiadavka po stále väčšej šírke pásma je neutíchajúca a v poslednej dobe ešte zrýchľuje. Avšak zvýšená požiadavka po šírke pásma môže spôsobiť problémy s kvalitou.

QoS sa odkazuje na schopnosť siete poskytovať lepšie služby pre vybraný typ sieťovej prevádzky nad rozličnými podliehajúcimi prenosovými technológiami, zahrňujúc IP smerované siete, Frame Relay, ATM, Ethernet a 802.1 alebo Synchrónne optické siete (SONET/SDH). Vo všeobecnosti, QoS funkcie poskytujú lepšie a viac predvídateľné sieťové služby tak, že:

- Zlepšujú charakteristiky stratovosti
- Zabraňujú a riadia sieťové zahltenie
- Tvarujú sieťovú prevádzku
- Nastavujú prioritu sieťovej prevádzky naprieč sieťou

QoS môže zvýšiť šírku pásma pre časovo citlivé dáta a aplikácie, obmedziť šírku pásma pre nekritický sieťový prenos a poskytnúť konzistentnú sieťovú odozvu
Bez týchto QoS mechanizmov by mohli nepodstatné aplikácie veľmi rýchlo vyčerpať sieťové zdroje na úkor dôležitejších alebo priam kritických aplikácií, čo by obmedzilo firemné/nefiremné procesy a tým aj produktivitu.

IP siete sú koncipované ako best-effort siete. Lenže aplikácie pracujúce cez IP siete kladú rôzne nároky na kvalitu prenosu. Tak od začiatku komerčného využívania IP sietí sa začínalo zo štandardizáciou týchto poskytovaných služieb. Poskytovaním a zaisťovaním kvality služieb QoS sa zaoberá séria protokolov, ktoré sa delia na dve hlavné skupiny.

- IntServ pracuje na princípe, rezervácie prostriedkov pre dátové toky. Tento signalizačný protokol garantuje, že pred príchodom paketu na ďalší uzol bude mať pripravené adekvátne sieťové prostriedky na cestu sieťou k ďalšiemu uzlu. Takáto správa bola poskytovaná pre celý tok paketov.
- QoS model podľa DiffServ bol vytvorený IETF a je špecifikovaný v RFC 2474. DifServ oproti IntServ označuje každý paket a takto spravuje každý paket samostatne. To ponúka možnosť, že nebude garantovaná žiadna šírka pásma pre jeden konkrétny tok ako to je u IntServ služieb.

Pri meraní parametrov sa musí brať veľký ohľad na typ aplikácie, ktorá vyžaduje prístup sieti a jej následné využívanie. Je rozdiel akú kvalitu potrebuje aplikácia ktorá prenáša dáta (text, komprimovaný subor) alebo takzvané real-time applicatoins (hlas alebo internetovú televíziu). Preto sa služby vo všeobecnosti delia na tri skupiny a to služby VoIP, služby obrazového charakteru, a dátové služby.

DiffServ QoS Metódy:

Klasifikácia – väčšina QoS mechanizmov podporuje viacero tried. Existuje niekoľko klasifikačných nástrojov pre rôzne QoS mechanizmy (napríklad Access listy, smerovacie mapy alebo mapy tried). Každý triedovo-orientovaný QoS mechanizmus musí podporovať niektorý typ klasifikácie.

Metering – niektoré mechanizmy merajú množstvo sieťovej prevádzky na sieti a podľa týchto informácií sa potom zvolí adekvátna akcia (napríklad obmedzenie priepustnosti, shaping alebo sheduling).

Dropping – niektoré mechanizmy sa používajú na zahadzovanie paketov. Vyberie sa nejaká schéma pre zahadzovanie paketov rozdielna oproti bežnému tail-dropu pri preplnení fronty. Jedným z takýchto mechanizmov je WRED (Random early detection).

Policing – niektoré mechanizmy sú používané na limitovanie sieťovej prevádzky na základe údajov z meteringu tak, že pakety ktoré sú nad rámec stanoveného limitu sa zahodia. (napríklad CAR – Commited Access Rate)

Shaping - niektoré mechanizmy sú používané na limitovanie sieťovej prevádzky na základe údajov z meteringu tak, že pakety ktoré sú nad rámec stanoveného limitu sa oneskoria. (napríklad GTS)

Marking – niektoré mechanizmy majú schopnosť značkovať pakety na základe klasifikácie alebo meteringu. (napríklad CAR alebo class-based marking, pomocou IP precedencie alebo DSCP).

Queuing – niektoré mechanizmy sú používané pre radenie do frontov na výstupných rozhraniach. (napríklad CQ, PQ, WFQ, CBWFQ alebo IP RTP Priority)

Forwarding – existuje niekoľko podporovaných forwarding mechanizmov. (Process switching, fast switching alebo Cisco express forwarding)

5.1 QoS pre VoIP

Kvalitné spracovanie služby VoIP si kladie v súčasnosti najväčšie nároky na prenosovú sieť. Samotná služba sa skladá z dvoch typov dátového prenosu a to zo samotného prenosu telefónneho hovoru a z prenosu signalizačných informácií. Obyčajne VoIP je spracovávané najprv z celkového dátového toku. Požiadavky na sieť pre VoIP sú:

- Straty by nemali presiahnuť 1% z celkového počtu prenesených paketov
- Oneskorenie v jenom smere by nemalo presiahnuť 150 ms.
  Maximálne doporučené oneskorenie podľa ITU G.114
  - 0 – 150 ms - akceptovateľné pre bežné hovorové užívateľské aplikácie
  - 150 – 400 ms - akceptovateľné pre medzinárodné hovory
  - nad 400 ms obecne nie je možné tolerovať
    Avšak vždy ako u všetkých parametrov do hry vstupuje ľudský faktor a subjektívne hodnotenie latencie prenosu.
- Kolísanie oneskorenia (jitter) by malo byť pod 30ms.

Požiadavky na šírku pásma pri prenose hovoru cez dátovú sieť sú dané typom použitého kodeku, objemom režijných informácií a protokolmi, ktoré sú použité na prenos hlasu.

5.1.1 RTP Real-Time Transport Protcol

Nadviazanie komunikácie medzi dvomi účastníkmi sa deje v dvoch fázach. V prvej fáze sa pomocou signalizačných protokolov dohodne celý proces komunikácie. Teda aké kodeky sa použijú atď., a potom sa v druhej fáze použije dohodnutý dátový protokol, ktorým sa realizuje samotná dátová komunikácia.

Jedným z transportných protokolov je Real-Time Transport Protocol (RTP). Je to protokol, ktorý nezaručuje samotné doručovanie paketov a ani doručovanie správnom poradí, ale definuje ich poradové čísla a tak multimediálne aplikácie môžu rozpoznať ich nesprávne poradie a chýbajúce pakety. RTP najčastejšie používa UDP protokol.
RTP protokol bol navrhnutý pre individuálne, skupinové prenosy, pre jednosmerný ale aj obojsmerný prenos. Je tak použiteľný pre videokonferencie pre VoIP a používajú ho protokoly SIP a H.323.

K multimediálnemu obsahu RTP pripojuje hlavičku ktorá obsahuje poradové číslo paketu (sequence number), označenie typu obsahu (payload identification), označenie začiatku a konca rámca (frame indication), identifikácia zdroja (source identification), a synchornizáciu(intramedia synchronization)

5.1.2 Real-Time Transport Control protocol

Ako bolo povedané tak RTP protokol nezaručuje správne doručenie paketov. Správne doručovanie je monitorované pomocou podporného riadiaceho protokolu RTCP.
RTP Control Protocol je založený na periodickom vysielaní kontrolných paketov všetkým účastníkom videokonferencie. Používa pritom rovnaké distribučné mechanizmy ako dátové pakety s tým, že žiadne dáta neprenáša. Hlavnou úlohou RTCP je poskytovanie spätnej väzby QoS kde zbiera údaje o mediálnom spojení a informácie ako počet odoslaných bajtov, počet odoslaných paketov, počet stratených paketov, jitter. Podľa týchto informácií služba QoS je schopná upraviť parametre dátového spoja na kvalitnejší prenos.

5.1.3 H.323

H.323 je štandard ITU-T a bol vyvinutý v ”Enterprise LAN community“ ako video konferenčný protokol podobný signalizačným protokolom používaných v ISDN sieťach. Pôvodne bol určený pre vysokorýchlostné LAN siete, ktoré neposkytujú QoS. H.323 j tvorený sadou protokolov, ktoré samostatne vykonávajú určitú činnosť.
H323 architektúra pozostáva z nasledovných komponentov:

- Terminál
- Gateway
- Gatekeeper
- MCU *(Multipoint Control Unit)*

Táto architektúra bola v začiatkoch VoIP veľmi rozšírená ale vďaka jej nadmernej zložitosti a komplexnosti je v poslednej dobe vytlačovaná iným omnoho flexibilnejším protokolom a tým je Session Initiation Protocol – SIP

5.1.4 SIP Session Initiation Protocol

Session Initiation Protocol je internetový protokol určený na prenos signalizácie v internetovej telefónii. Obyčajne využíva UDP port 5060 ale môže fungovať aj na TCP protokolu s portom 5060. Ako už bolo povedané je to protokol slúžiaci na zaistenie spojenia. Dnes je najviac rozšíreným protokolom vďaka jeho jednoduchosti kde prenáša len to čo je potrebné.
SIP je tzv. request – response v dôsledku toho môže SIP bez problémov koexistovať s existujúcimi internetovými aplikáciami. Takto sa VoIP telefónia stáva ďalšou internetovou aplikáciou a ľahko sa integruje do iných internetových služieb.

5.1.5 Kodeky

Veľkosť šírky pásma, ktorú nám využíva hlasová komunikácia cez dátovú sieť, je možné ovplyvniť vhodným výberom spôsobu kódovania hlasu do digitálnej podoby. Pri kódovaní sa vyžíva nedokonalosť ľudského sluchu kde nie je potrebné prenášať 100% analógovej informácie. Pri kódovaní sa neprenášajú frekvencie, ktoré nie je možné ľudský sluch zaznamenať a ďalej sa využíva schopnosti mozgu domyslieť si chýbajúcu alebo nekompletnú informáciu.

kodek	Data bitrate (Kbps)	licencia
G.711	64	nie
G.726	16,24,32,40	nie
G.729A	8	áno
GSM	13	nie
iLBC	13.3 (30-ms frames) 15.2 (20-ms frames)	nie
Speedx	premenná (2.15 - 22.4)	nie

Tabuľka č.2 tabuľka kodekov

G.711 – využíva pulzovo kódovú moduláciu (PCM). Používa dve kódovacie metódy μlaw v Severnej Amerike a alaw mimo Severnej Ameriky. Prenáša sa 64 000 bitov za sekundu. Má minimálne požiadavky na CPU.
G.726 – využíva adaptívnu diferenciálnu pulzovo šírkovú moduláciu. Prenos sa deje na niekoľkých šírkach pásma. Je to z dôvodu, že namiesto posielania výsledku kvantizačného merania posiela len informáciu o popisu rozdielu medzi predchádzajúcou a súčasnou vzorkou.
G.729A – Využíva Conjugate-Structure Algebraic–Code–Excited Linear Predictions (CS-ACELP). V prípade tohto kodeku je budovaný tzv. codebook zvukov matematickou modeláciou rôznych ľudských hlasov. Namiesto toho aby sa posielala aktuálna vzorka hlasu pošle sa kód odpovedajúcej vzorky hlasu. Kvôli patentom sa tento kodek nemôže voľne používať. Týmto kodekom sa prenáša hlas rýchlosťou 8 000 bitov za sekundu.
GSM – poskytuje podobné parametre ako G.729A, s tým že je voľne použiteľný.
iLBC – the internet Low Bitrate Codec poskytuje zaujímavý mix kvality a využitie šírky pásma. Tento kodek je vhodné použiť na stratové pinky. Tento kodek do značnej miery zaťažuje CPU. Tento kodek bol vyvinutý spoločnosťou Global IP Sound.
Speex – Tento kodek dokáže zmeniť vzorkovaciu frekvenciu a tým aj šírku pásma podľa podmienok v sieti. Jeho prenosová rýchlosť je od 2,15 až 22,4 kbps.

5.1.6 MOS

Mean Opinion Score (MOS) sa bežne používa pre ohodnotenie kvalitu telefónneho rozhovoru vyjadrenú na stupnici od 1 do 5, kde 5 je najlepšia kvalita. Hodnotenie číslom 4 sa vo všeobecnosti považuje za kvalitu známu z dnešných PSTN/TDM sietí. MOS je funkcia mnohých faktorov, zahrňujúcich typ siete, použitý kodek, kabeláž a vybavenie a dokonca aj vstupné zariadenia, ktoré sa používajú (headsety).

MOS bol pôvodne určený na subjektívne sluchové testovanie, kde sa skupina trénovaných expertov pokúšala hlasovej vzorke priradiť nejakú priemernú hodnotu. Testovacie vybavenie dnes vypočítava MOS použitím sofistikovaných algoritmov, ktoré sú navrhnuté aby veľmi presne aproximovali výsledky subjektívnych sluchových testov. MOS je celkové ohodnotenie hlasovej kvality, zahrňujúc tucty faktorov do jedného výsledného skóre. Pretože je to ale všeobecná mierka odzrkadľujúca mnoho faktorov, nemalo by sa MOS používať ako výhradné hodnotenie hlasovej kvality. Niektoré faktory ako echo, oneskorenie alebo sila hovoru by pri istých algoritmoch MOS skóre výrazne neznížili avšak subjektívny pocit z hovoru by sa zhoršil výrazne. Najlepšie hodnotenie kvality preto pozostáva z monitorovania jednotlivých faktorov hlasu ako je šum, oneskorenie, jitter a strata paketov spolu s hodnotením MOS pri použití viacerých algoritmov.

Existuje niekoľko štandardizovaných MOS algoritmov, každý pôvodne navrhnutý pre konkrétne použitie. Niektoré algoritmy spracúvajú iba štatistiky založené na paketovom prenose (IP), kde iné zahŕňajú aj analógové merania ako je šum, hlasitosť, echo a skreslenie aby sa zvýšila presnosť a opakovateľnosť. Pretože ucho je analógové zariadenie a zvuk je analógový signál, je dôležité zahrnúť do výsledkov aj túto analýzu. MOS ohodnotené použitím IP aj analógových meraní omnoho presnejšie vystihuje subjektívny pocit z hovoru.

PESQ ITU T P.862
P.563 Listening MOS
VQES Algoritmus
RTCP & RTCP-XR - IETF RFC-3611
E-Model G.107, 108, 109

5.2 QoS pre video prenosy

Video prenosy môžeme rozlíšiť na dva typy aplikácií a to interaktívne video a streamované video kde nároky na prenosovú sieť sa líšia.
Pre interaktívne video alebo aj videokonferencia sú kladené tieto požiadavky:

- Stále parametre prenosu. Teda rovnaká miera strát, rovnaké oneskorenie atd.
- Straty by nemali presiahnuť 1% z celkového počtu prenesených paketov
- Oneskorenie v jenom smere by nemalo presiahnuť 150 ms.
- Kolísanie oneskorenia (jitter) by malo byť pod 30 ms.

Rýchlosť potrebná na prenos interaktívneho videa je udávaná na 384 kb/s^{-1}, ale obyčajne a na prenos rezervuje 460 kb/s^{-1}. Je to dané premenlivou jednak premenlivým objemom dát a hlavne kolísavým nárastom riadiacich dát, či video a lebo audio zložky, ktorých objem môže narásť až na 20% celkového objemu prenesených dát.

Streamované video má oproti interaktívnemu videu miernejšie požiadavky na prenos

- Straty by nemali presiahnuť 5% z celkového počtu prenesených paketov

- Oneskorenie by nemalo presiahnuť 4 – 5 sekúnd
- Streamované video nemá výrazné požiadavky na jitter
- Šírka pásma je závislá od použitého kodeku a rýchlosti streamovaného videa
- Dátový prenos streamovaného videa obyčajne ide jedným smerom tak požiadavky na prenos je len jedným smerom a to k užívateľovi.

Táto služba nie je citlivá na oneskorenie a tak na strane prijímača môže byť nastavená väčšia vyrovnávacia pamäť na vyrovnanie kolísania dátovej prevádzky.

Pre video hovory sa používa najmä H.261 a H.263
H.261 – je štandard kódovania videa pôvodne určený pre prenos cez ISDN, na ktorých sú prenosové rýchlosti násobkami 64 kbps. Rýchlosť prenosu dát z kódavacieho algoritmu bol navrhnutý tak aby kodek mohol pracovať v rozmedzí rýchlostí 40kbps až 2Mbps. Tento štandard podporuje rámcové veľkosti CIF a QCIF
H.263 – Tento kodek bol vyvinutý z kodeku H.261a je primárne určený pre videokonferencie.

5.3 QoS pre dátové prenosy

Táto kategória patrí medzi najväčšiu a najrozmanitejšiu skupinu sieťových aplikácií. Charakter ich komunikácie, objem prenášaných dát a tak aj požiadavky na sieťové prostriedky sú značne rozmanité. Dátové prenosy sa obyčajne delia na štyri hlavné skupiny.

Best-Effort dáta

Toto je základná skupina kde sa zaraďuje všetok dátový prenos. Len ak aplikácia vyžaduje iné požiadavky je presunutá do inej skupiny. Tento prenos obyčajne pokrýva 25% šírky pásma.

Bulk dáta

Tu patria aplikácie, ktoré nie sú interaktívne dokážu eliminovať straty a ich prenos má dlho trvajúci charakter. Typickým predstaviteľom je služba FTP, zálohovanie atď. Správanie týchto aplikácií zaradených v tejto skupine je taký, že môžu dynamicky zaberať šírku pásma podľa intenzity prevádzky.

Transakčné a interaktívne dáta

Trieda transakčných a interaktívnych služieb zahrňuje dva podobné typy aplikácií, transakčné aplikácie typu klient/server napríklad SAP, Oracle, atď. a interaktívne komunikačné služby typu, ICQ, Netmeeting, atď. Rozdiel medzi klasickými a transakčnými službami typu klient/server je predovšetkým v obmedzení na oneskorenie. U týchto služieb obyčajne prebieha komunikácia medzi človekom a strojom, kde pohodlná obsluha vyžaduje dostatočne rýchlu odozvu.

Užívateľsko-špecificky kritické služby

Toto predstavuje dáta a služby, ktoré sú kľúčové pre chod danej organizácie. Ide obyčajne o transakčné a interaktívne dáta, ktoré majú byť ešte viacej uprednostňované. Typ dát a služieb sa líši od organizácie. Očakáva sa v tejto skupine je zaradených len málo takýchto aplikácií.

6 Parametre dátových sietí

6.1 Oneskorenie (latency)

Oneskorenie je čas, ktorý uplynie od odoslania správy daným uzlom po prijatí na cieľovom uzle. Je potrebné rozlíšiť oneskorenie jednosmerné (čas medzi odoslaním paketu zdrojom a jeho prijatím cieľovou stanicou) a oneskorením obojsmerným tzv. round-trip latency, ktorý zahŕňa cestu paketu tam aj späť plus čas jeho spracovania cieľom. Toto oneskorenie (inak nazvané round-trip time RTT) sa najčastejšie používa k meraniu, lebo je ho možné merať z jednej stanice.

Je to jeden z najdôležitejších QoS parametrov. Tento parameter má najväčší vplyv na služby pracujúce v reálnom čase. Oneskorenie úzko súvisí so všetkými parametrami kvality prenosu dát. Obyčajne medzi kvalitou a oneskorením býva priama úmera. Celkove oneskorenie môžeme brať ako súčet týchto časov:

- Doba zostavenia aplikačného rámca
- Oneskorenie spôsobené zostavením paketu
- Oneskorenie spôsobené prekladaním
- Oneskorenie spôsobené zabezpečovaním informácií
- Doba šírením médiom
- Doba spôsobená čakaním paketu vo fronte vytváranej v sieťoých uzloch
- Oneskorenie spôsobené tvarovaním prevádzky
- Onekorenie spôsobené vyrovnávaním kolísania oneskorenia

Doba zostavenia aplikačného rámca vychádza zo sekvenčného spracovania dát a je spôsobená zdrojovým kódovaním tak že musí spracovať určitý úsek signálu.

$$t_f = \frac{\mathrm{n_s}}{f_\mathrm{s}}$$

- t_f – dĺžka trvania rámca
- n_s – počet vzorkov v rámci
- f_s – vzorkovacia frekvencia

Doba zostavenia aplikačného rámca

Oneskorenie spôsobené zostavením paketu je spôsobené čakaním na dostatočné množstvo dát a to je ovplyvnené veľkosťou paketu a potom vytváraním hlavičky.

$$oneskorenie\ paketizácie = \frac{\mathrm{N}}{v_\mathrm{p}}$$

- N – veľkosť poľa payload ppaketu alebo bunky [bits]
- v_p - prenosová rýchlosť [kb/s]

Oneskorenie spôsobené prekladaním. Prekladanie odstraňuje prípadné zhluky chýb spôsobené prenosom.

$$t_p = \frac{(\mathrm{n.m.l})^2}{\mathrm{r}}$$

- n – počet prekladaných rámcov
- m – počet vzoriek v rámci
- m – počet bitov v jednej vzorke
- r – bitová rýchlosť kodeku

Oneskorenie spôsobené zabezpečovaním sekvencie je závislé na požitej zabezpečovacej metóde a tým na algoritme akú ta metóda využíva. Obyčajne platí pravidlo čím vyššie zabezpečenie dát tým je potrebné viac času na zašifrovanie a potom následné dešifrovanie.

Oneskorenie spôsobené dobou šírením signálu médiom. Toto oneskorenie je prirátavané k celkovému oneskoreniu najmä pri komunikácii na väčšie vzdialenosti.

$$t = \frac{\mathrm{l}}{\mathrm{c}}$$

- l – dĺžka trasy
- c – rýchlosť šírenia svetla v vákuu

Na presnejší odhad je potrebné uvažovať aj vplyv materiálu, z ktorého je médium vytvorené.

Doba spôsobená čakaním paketu vo fronte je spôsobená aktívnymi prvkami prenosovej siete. Detailnejším riešením oneskorenia a jeho optimalizácie sa zaoberá teória front.

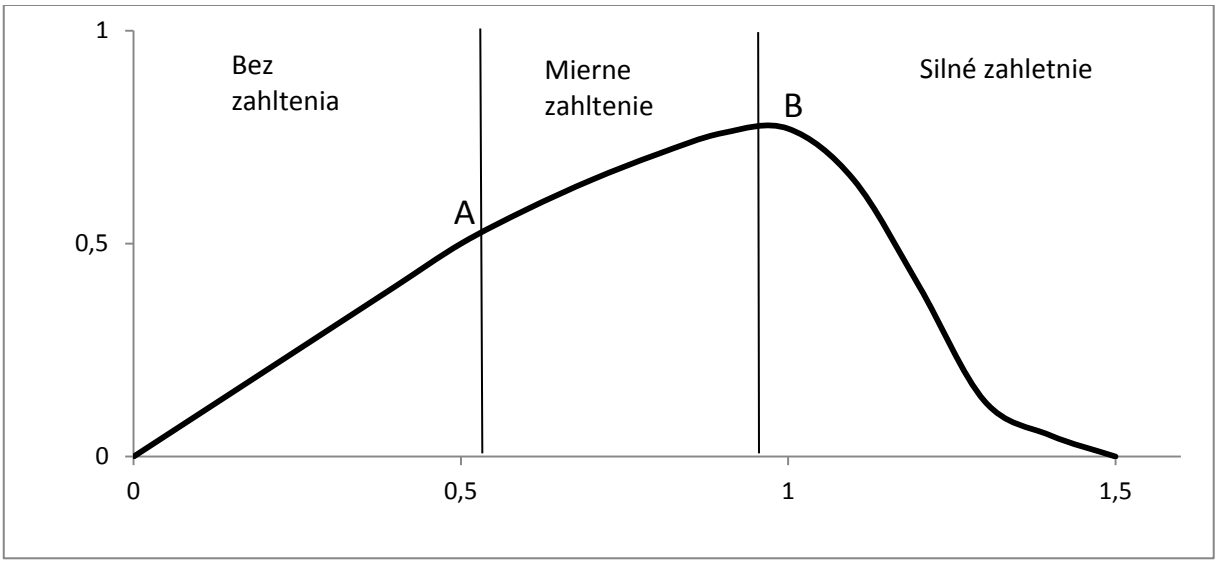
Oneskorenie spôsobené vyrovnávaním kolísania oneskorenia. Jitter alebo kolísanie oneskorenia zásadne ovplyvňujú tzv. „real time“ služby ako je prenos hlasu a videa. Pre zníženie kolísania oneskorenia, prichádzajúce pakety na prijímacom konci sú časovo vyrovnávané v tzv. jitter vyrovnávacej pamäti, z ktorej vystupujú s konštantou rýchlosťou a tým aj oneskorením. Obyčajne toto oneskorenie v buffery pre vyrovnanie jeho kolísania dosahuje hodnotu okolo 60ms.

6.2 Priepustnosť

Priepustnosť siete sa vzťahuje k objemu údajov, ktoré môžu prechádzať prostredníctvom siete. Priepustnosť siete je ovplyvnená rôznymi faktormi, ako sú používané protokoly, možnosti smerovačov a prepínačov, typ kabeláže, ako je Ethernet alebo optické vlákna, ktoré sa používajú na vytvorenie siete.

Oneskorenie spôsobené tvarovaním prevádzky. Toto oneskorenie sa aktívne podpisuje pri riadení priepustnosti. Kľúčom pri riadení priepustnosti je aby nedošlo k zahlteniu sieťových prvkov. Preto boli vyvinuté rôzne algoritmy, ktoré majú

predpovedať a následne eliminovať takéto zahltenie. V globálnom meradle môžeme paketovú prenosovú sieť považovať za sieť front. Všetky sieťové prvky sú vybavené pamäťou kde sa ukladajú pakety, ktoré nemôže systém aktuálne spracovať. V prípade ak pakety prichádzajú rýchlejšie než je možné ich spracovať dochádza k zaplneniu pamäte aktívneho prvku a tým aj k nárastu oneskorenia a konečnom prípade aj strate paketu.
Na obrázku je znázornené chovanie reálnej siete bez réžie prenosu dát a nekonečnou frontou.



Graf č.1 graf priepustnosti

Ako je vidieť pri nízkom zaťažení priepustnosť a vyťaženosť narastá so zvyšujúcim zaťažením. Po dosiahnutí bodu A už nárast priepustnosti nebude priamo úmerná zaťaženiu. Po tomto bode sa sieť dostáva do stavu mierneho stavu zahltenia. Ďalším nárastom záťaže narastajú fronty v uzloch a sieť sa rýchlo dostáva do stavu silného zahltenia kde už dochádza aj k zahadzovaniu paketov. Druhý graf ukazuje exponenciálny nárast oneskorenia.
Pri riadení priepustnosti je kladený dôraz na riadení priepustnosti pri zahltení tj. Efektívne využívanie siete pri väčšom zaťažení. Z toho vyplývajú ďalšie požiadavky ako sú:

- Spravodlivosť – rovnaký dopad na každý dátový tok
- Zaistenie kvality služieb – riadená diferencializácia spracovania prevádzky
- Rezervácia sieťových zdrojov – dohľad nad prichádzajúcou prevádzkou

Algoritmy, ktoré zabraňujú zahlteniu sú:

- Backpresure (spätný tlak)
- Chocke paket (tlmiaci paket)
- Implicitná signalizácia zahltenia
- Explicitná signalizácia zahltenia

6.2.1 Riadenie priepustnosti u protokolu TCP

U protokolu TCP sa riadenie priepustnosti spravuje pomocou techniky posuvného okna. To umožňuje prijímaču podľa potreby krokovať vysielač v posielaní rámcov. To sa deje na základe spätnej väzby kedy prijímač odošle potvrdenie o príjme spolu ostatými informáciami, ktoré pomáhajú vysielaču analyzovať sieť a tak prispôsobiť svoje odosielanie.
Vďaka tejto komunikácii môže protokol dynamicky meniť svoju prenosovú rýchlosť. Od zavedenia protokolu TCP bola navrhnutá a implementovaná celá rada mechanizmov riadenia priepustnosti pre TCP. Najbežnejšie mechanizmy sú:

- RTT Variance Estimation (odhad kolísania doby odozvy)
- Exponential RTO Backoff (exponenciálne predlžovanie doby časovača opakovaného vysielania)
- Karn's algorithm (Karnov algoritmus)
- Slow Start (pomalý štart)
- Dynamic Window Sizing on Congestion (dynamické nastavenie veľkosti okna v prípade zahltenia)
- Fast Retransmit (rychly opakovaný prenos)
- Fast Recovery (rychle zotavenie)

6.3 Chybovosť

Chybovosť je ďalší parameter, ktorý sa výrazne podpisuje pod kvalitu prenosu v dátových sieťach. Jedná sa počet stratených paketov verzus počet prijatých paketov. Chybovosťou sa zaoberá riadenie chybových stavov a ma na starosti riešenie straty alebo poškodenia dátovej jednotky počas prenosu od odosielateľa k príjemcovi. Obyčajne sú implementované algoritmy na detekciu chýb s využitím kontrolného súčtu Frame check Sequence – FCS a opakované vysielanie dátovej jednotky. Väčšinou mechanizmy riadenia toku dát a riadenia chybových stavov sú implementované do jedného spoločného mechanizmu, ktorý reguluje tok dátových jednotiek a rozhoduje o opakovanom vysielaní.

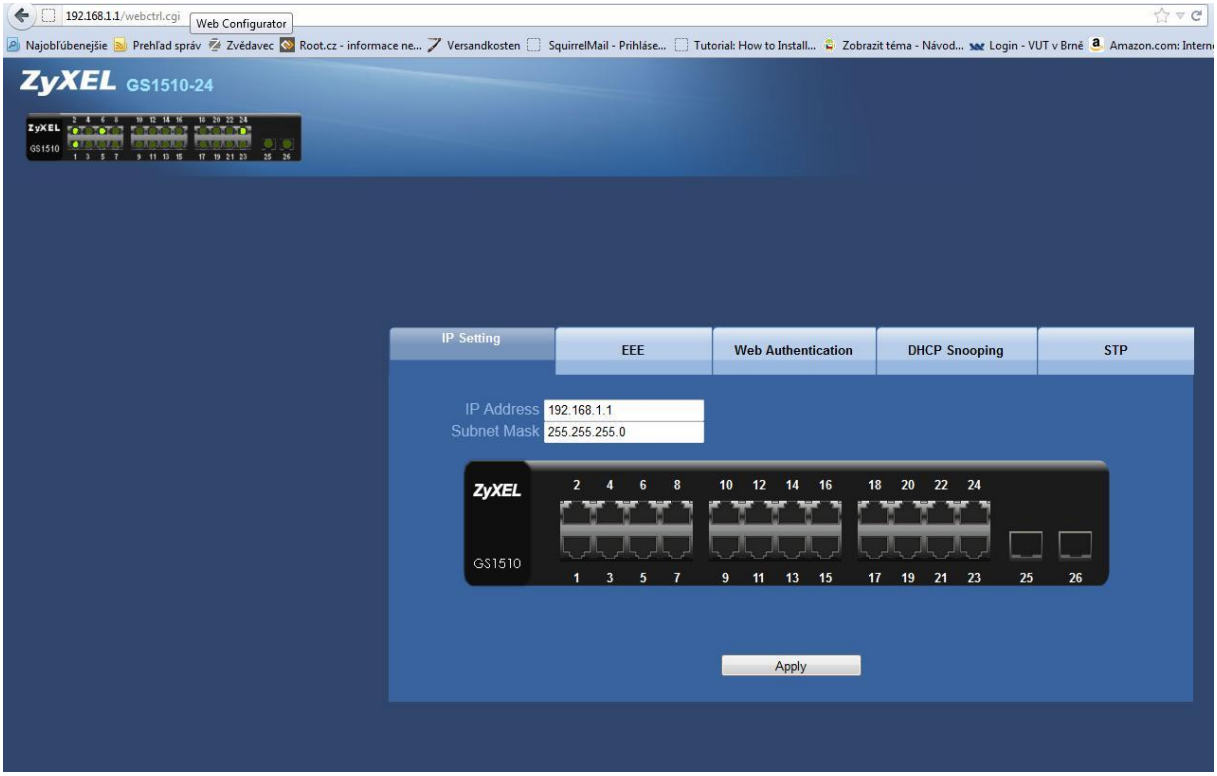
Existujú tri mechanizmy, ktoré sa bežne využívajú:

- Stop-and-wait (stoj a čakaj)
- Go-back-N (návrat o N)
- Secective-reject (selektívne zamietnutie)

7 Meranie parametrov

Obecne povedané sieťová administrácia sa týka aktivít týkajúcich sa chodu aktivít siete a s tým aj technologická podpora týchto aktivít. Veľká časť riadenia siete pozostáva zo sledovania a porozumenia chodu siete.
Sieťová administrácia zahŕňa niekoľko činností a to sú sledovanie, údržba, administrácia a v každej z nich sa pracuje s parametrami siete či už výkonnostnými alebo kvalitatívnymi.
Cieľom získavania a spracovávania týchto parametrov je udržiavanie stálosti parametrov a následné zvyšovanie kvality služieb poskytovaných užívateľom sietí. Ďalšia funkcia sieťovej administrácie je, ako už bolo spomenuté, zaznamenávanie parametrov siete a vyhodnocovanie a predpovedanie krízových situácii a následné zamedzenie vzniku takýchto situácií.
Kvalitne nastavená sieťová administrácia umožňuje v budúcnosti implementáciu nových technológií a služieb.

Nástroje na monitorovanie sietí môžeme rozdeliť na niekoľko častí. Toto delenie je organizované podľa typu a objemu dát, ktoré z týchto nástrojov získame. Vo väčšine prípadov jedná o aplikácie.
Prvý z nich sú takzvané *craft terminals*. Obyčajne ukazujú grafické zobrazenie skutočného zariadenia , ktoré sa zobrazí po vzdialenom pripojení väčšinou fungujúce cez webový prehliadač. Ako je vidno z obrázka zobrazuje základné parametre ako je stav zariadenia, stav jednotlivých portov.



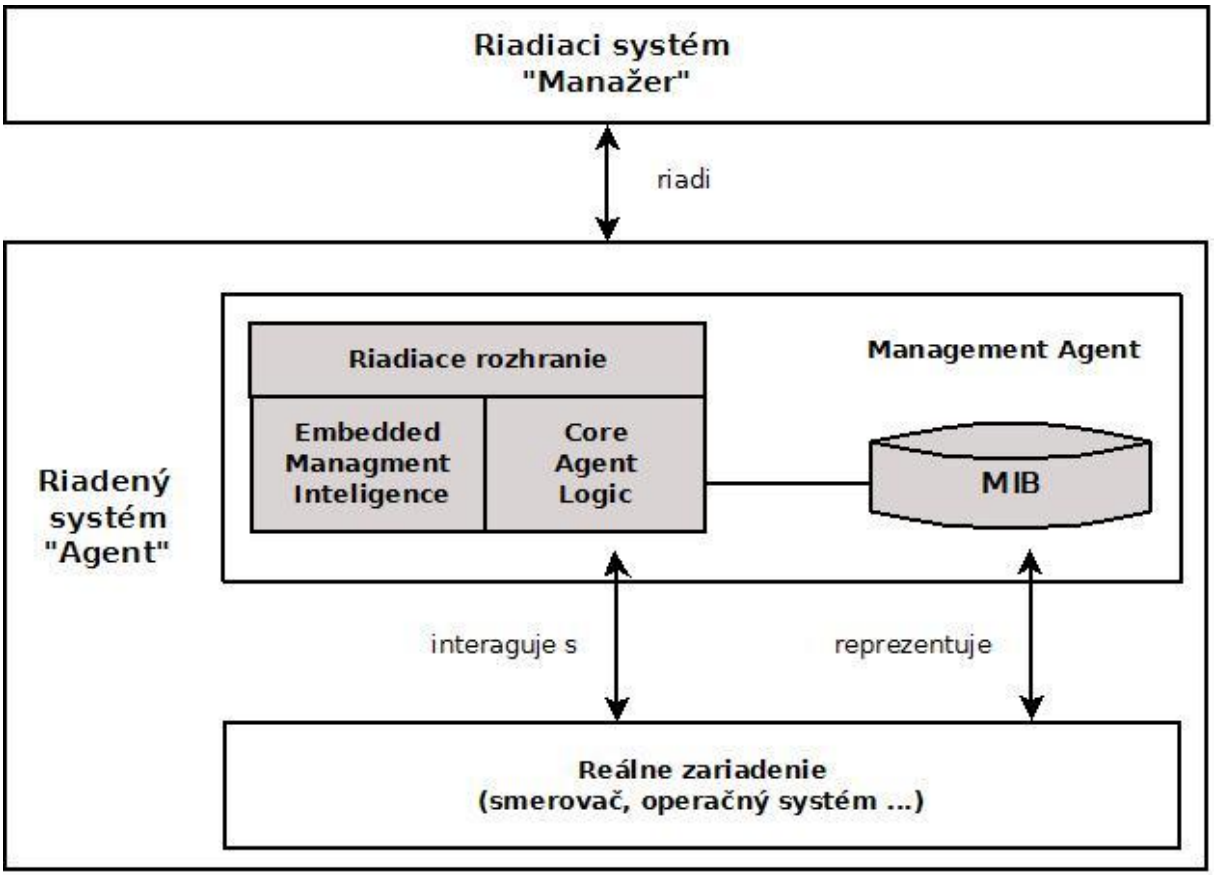
Obr.5 zobrazenie craft terminála

Sieťové analyzátory, ktoré monitorujú aktuálnu prevádzku v sieti, jej chovanie. To je dôležité na riešenie problémov vznikajúcou počas prevádzky. Sieťové analyzátory odchytávajú pakety na portoch zariadení alebo na koncových staniach a predávajú hodnoty paketu na ďalšiu analýzu.
Správa komponentov je nástroj, ktorý je tak povediac nadstavbou craft terminálov. Tu je možnosť nastaviť parametre jednotlivých zariadení zálohovanie týchto parametrov.
Kolektory a sondy sú nástroje na získavanie hodnôt parametrov z dátových sietí. Jedným zástupcom je Netflow vyvinutým spoločnosťou Cisco. Tento protokol zaznamenáva prevádzku siete zo smerovačov.

Sondy fungujú na podobnom princípe ako kolektory len s tým rozdielom, že pracujú aktívne. Teda v určitých okamžikoch spúšťajú rôzne akcie na sieti a následne získava odozvu od takýchto udalostí.
Systémy analýzy výkonnosti umožňujú užívateľom analyzovať prevádzku a stanoviť tak možné chovanie siete pri budúcich udalostiach. Tieto systémy spracovávajú veľké množstvá dát a následne ich spracovávajú dáta do formy, ktoré sú použiteľné na ďalšie spracovanie užívateľom.

7.1 Popis zariadenia manažéra

Pri spracovávaní údajov z dátových sietí vystupujú zariadenia ako zariadenia ktoré sledujú sieť a sa nazývajú manažéri (client) a zariadenia, ktoré sú sledované a tie sa volajú agenti. Princíp je znázornený na obrázku kde zariadenie, ktoré sleduje stav je označované ako klient a zariadenie, ktoré je sledované je značené ako server. Ale v prípade sledovania siete je stav taký, že malé množstvo manažérov sleduje veľké množstvo agentov kde v situácii klient server je to opačne.
Dôležitou časťou manažéra je takzvaný riadiaci agent (Management Agent). Táto aplikácia má na starosti samostatnú komunikáciu medzi riadiacou jednotkou (manažér) a agentom, ukladá a spracúva dáta. Skladá sa z troch častí riadiace rozhranie, riadiaca informačná základňa (Management Information Base MIB) a (Core Agent Logic CAL).



Obr.6 zobrazenie interakcie manažéra a agenta

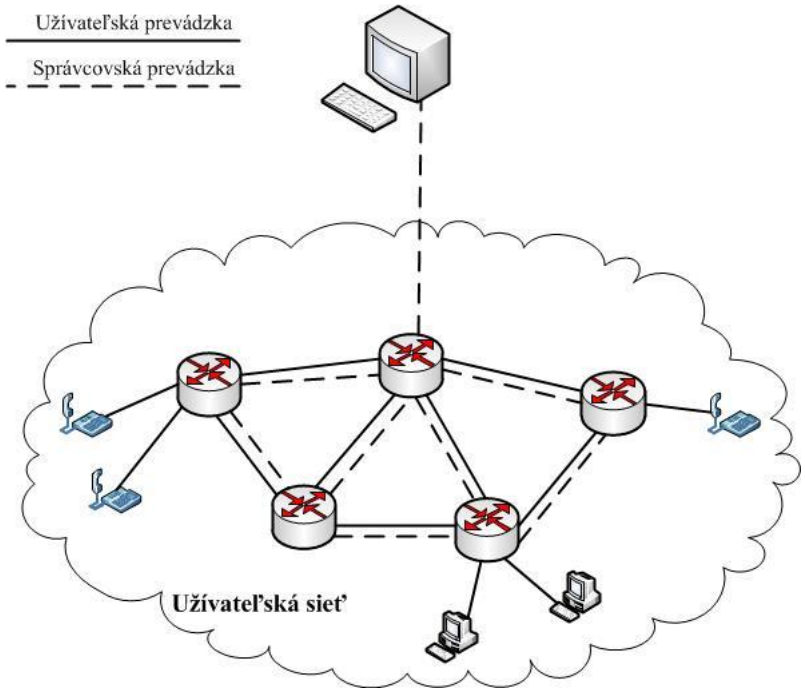
Riadiace rozhranie – zabezpečuje riadiacu komunikáciu
riadiaca informačná základňa (MIB) - úložisko dát, ktoré obsahujú dáta riadeného zariadenia
Jadro logiky agenta (CAL) – sprostredkováva komunikáciu medzi zariadením a MIB

Riadiaci agent je súčasťou smerovačov a prepínačov. Riadiace systémy alebo systémy na získavanie parametrov zo siete môžeme zaradiť do riadiacej siete (management network MN). Táto riadiaca sieť môže bežať na rovnakých fyzických cestách ako užívateľská sieť alebo môže byť vystavaná paralelná sieť, ktorá slúži len na správu užívateľskej časti. Na rozdiel od užívateľskej prevádzky riadiaca prevádzka má priamy vplyv na spravovaný objekt, kde oproti tomu užívateľská prevádzka len prechádza cez jednotlivé prvky k svojmu cieľu bez nejakej zmeny daného zariadenia.
Pri získavaní požadovaných informácií o sieti je potrebné sa pripojiť na dané zariadenie na ktorom beží systémový agent. Môžeme sa pripojiť tromi spôsobmi.
Priamo cez sériový port. U tohto spojenia je potrebná fyzická prítomnosť u daného zariadenia.
Druhá možnosť je prepojiť zariadenia s terminálovým serverom pomocou sériového rozhrania. Každé sériové pripojenie je označené číslom portu na rozlíšenie pripojeného zariadenia. Ďalej je terminálový server pripojený k sieti Ethernet obyčajne pomocou Fast Ethenetoveho portu. Terminálový server má obyčajne pridelenú IP adresu.

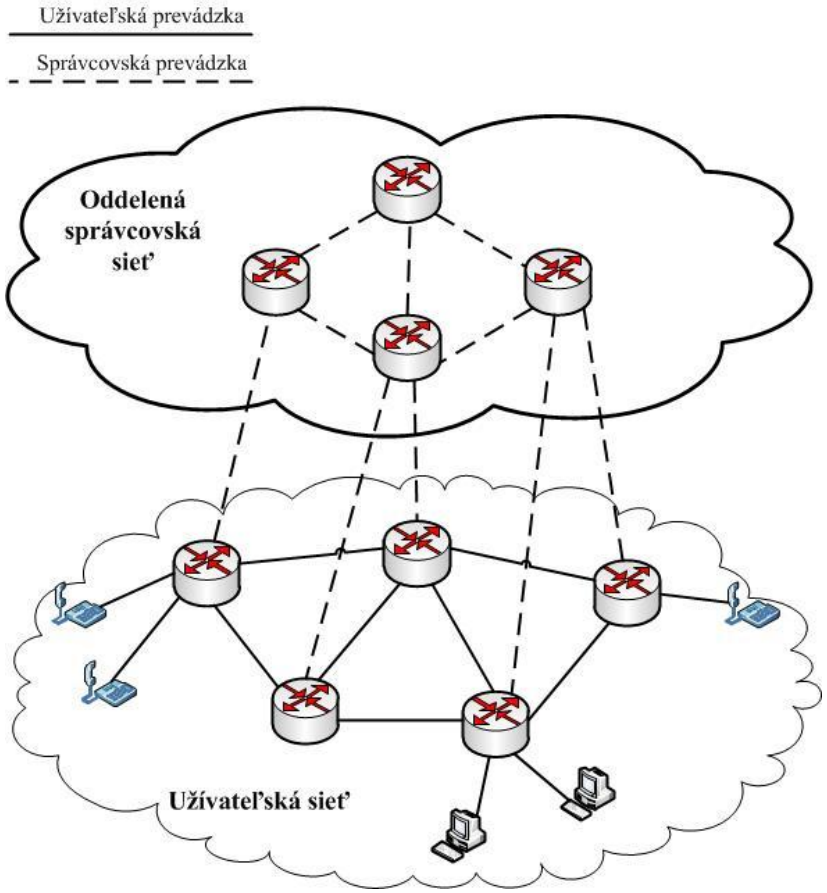
Tretia možnosť je pripojenia sa na dané zariadenie pomocou Ethernetového portu. Sieťové zariadenie má svoju IP adresu a tak po zadaní IP adresy požadovaného zariadenia dané zariadenie pracuje ako host teda koncové zariadenie. Tu môže byť port vyhradený len nariadiacu sieť (managemant network) alebo riadiaca sieť je prevádzkovaná na užívateľskej sieti kde je riadiaca sieť paralelne v prevádzke spolu s užívateľskou sieťou.

Po pripojení sa pracuje cez manager agenta pomocou CLI (Command Line Interface).Pomocou CLI je možné získať potrebné údaje alebo dokonca meniť nastavenie zariadenia.

Pri meraní parametrov je dôležité ako je daná sieť vytvorená. Tak ako bolo spomínané je možné riadiacu sieť prevádzkovať spolu s užívateľkou sieťou na tých rovnakých kábloch. Schéma zapojenia je na Obr.7. Alebo mať riadiacu sieť oddelenú od užívateľskej siete tieto siete pracujú paralele a nezávisle na sebe tak ako je vidno na obr.8.



Obr.7 zobrazenie paralelné prepojenie riadiacej siete a užívateľskej siete



Obr.8 zobrazenie oddelenia riadiacej siete a užívateľskej siete

Každá z týchto variant má svoje výhody na nevýhody z hľadiska ďalších možností využitia. Pri pohľade na získavanie parametrov siete či už sa jedná o kvalitu alebo výkon variant s oddelenými sieťami je efektívnejší z dôvodu menšieho vplyvu riadiacej prevádzky na výsledné dáta.

7.2 Spôsoby získavania parametrov z dátových sietí

Existujú tri hlavné dôvody prečo je dôležitá oblasť správy a merania parametrov dátových sietí.

- Riešenie sieťových problémov (troubleshooting). V sieti vznikajú rôzne situácie kedy je narušená funkčnosť dátovej siete. Môže sa jednať o chybné zariadenie, nesprávna cieľová adresa, bezpečnostné útoky atď. V takýchto situáciách podrobná analýza nameraných hodnôt dokáže lokalizovať problém a zjednodušiť jeho odstránenie.
- Vylaďovanie protokolov. Vývojári často chcú otestovať nové verzie aplikácií alebo protokolov a systém správy a merania sietí dokáže poskytnúť adekvátnu spätnú väzbu vývojárom aký má daná aplikácia vplyv na sieťovú prevádzku a jej správanie.
- Meranie výkonnosti. To slúži na určenie ako dobre stávajúci protokol alebo aplikácia pracuje v sieti. Detailná analýza pomáha určiť výkonnostné prekážky. Tak sa aj správa sieti podieľa na vývoji nových protokolov a aplikácií.

Dole sú rozpísané spôsoby ako sa parametre a iné relevantné informácie môžu získať z dátových sietí a každá má svoj protiklad:

Aké zariadenie je požité na zaznamenávanie dát. To môžeme rozdeliť na dve skupiny. Meranie je spracovávané špecializovaným zariadením tzv. analyzátormi dátovej prevádzky. Tieto zariadenia bývajú obyčajne dosť nákladné. Oproti tomu meranie ktoré je spracovávané softwarovo. Jedná sa o aplikáciu, ktorá obyčajne je spustená na niektorej stanici v meranej sieti. Táto stanica je mierne upravená na odchytávanie paketovej prevádzky. Takéto softwarové nástroje sú oveľa lacnejšie, ale vyrovnajú sa výkonu a funkciám hardwarových zariadení na meranie prevádzky.

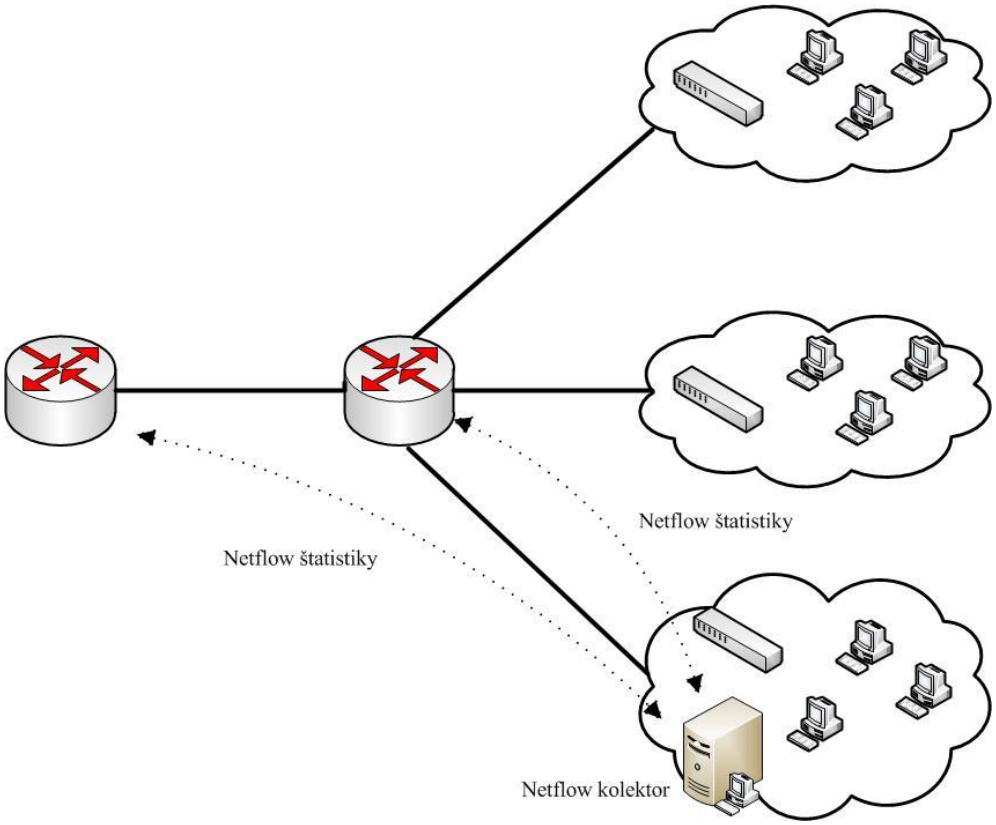
Ďalšími metódami merania prevádzky je delenie podľa prístupu:
Pasívny alebo aktívny prístup merania. Pasívne meranie je založené len na pozorovaní a zaznamenávaní stávajúcej prevádzky bez aktívneho zasahovania alebo vkladania vlastnej sieťovej prevádzky. Väčšina meracích nástrojov spadá do tejto kategórie.
Oproti tomu aktívne meranie je založené na merané prevádzky, ktorá sa vytvorila a vniesla do siete len za účelom merania. Príklad takéhoto aktívneho merania je spustenie príkazu ping. Tu sa vytvorí prenos niekoľkých testovacích paketov na kontrolu pripojenia a oneskorenia (latency) medzi dvomi stanicami.

Ďalšie delenie je podľa spôsobu spracovania. Teda na spracovávanie v reálnom čase a dodatočné spracovávanie. Pri spracovávaní v reálnom čase sú práve prebiehajúce dátové toky a ich údaje spracovávané a hneď predávané administrátorovi na analýzu. Spracovávané údaje s môžu zobraziť vo forme grafov alebo tabuliek. V jednoduchosti je vidno aktuálne dianie na sieti. Väčšina hardwarových analyzátorov je schopná spracovávať dátové toky v reálnom čase. Druhý spôsob je ten, že sa najprv dáta zo sledovania sieťovej prevádzky ukladajú a potom sa následne spracovávajú a vyhodnocujú. Príklad tohto spracovania môže byť spracovanie záznamov (logov) týždennej prevádzky na ftp serveru.

7.3 Netflow

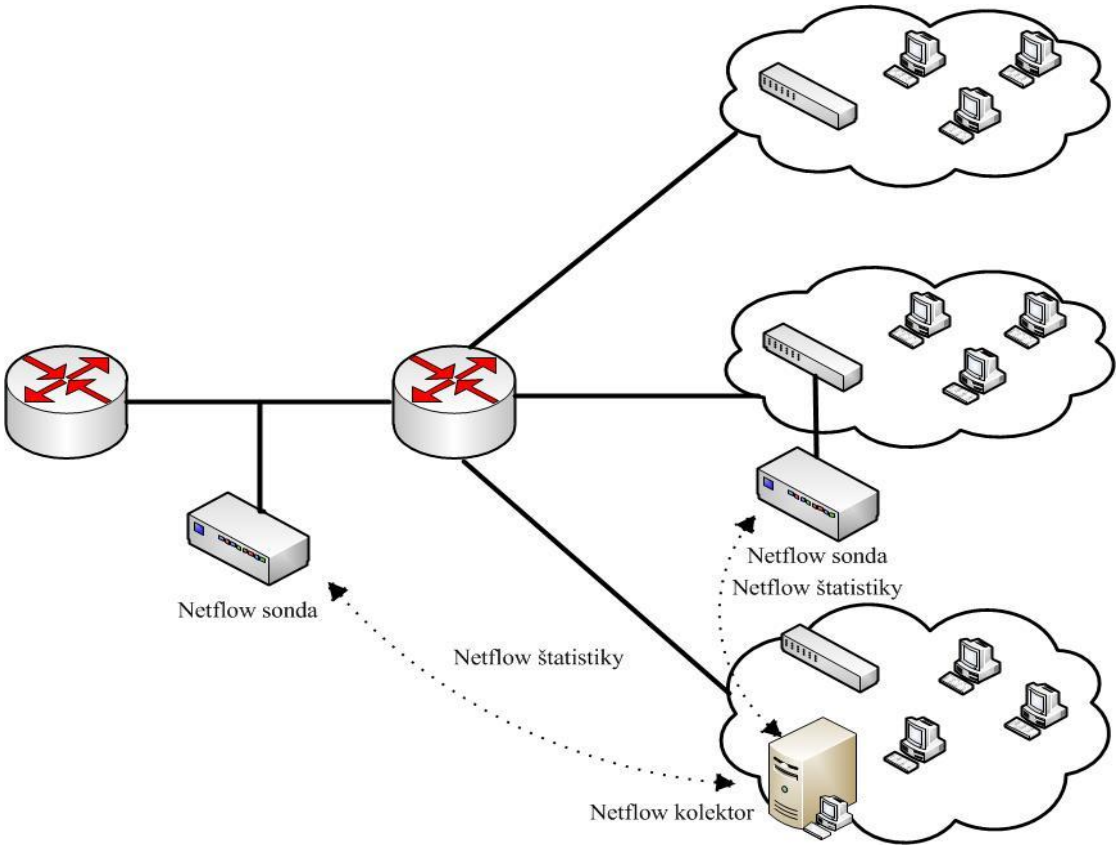
Netflow bol pôvodne vyvinutý ako doplnková služba k Cisco smerovačom Je to sieťový protokol vyvinutý spoločnosťou Cisco Systems . Jeho účelom je monitorovanie sieťovej prevádzky na základe IP tokov. Takto sieťový administrátori majú prehľad nad sieťovou prevádzkou v reálnom čase. Pomocou Netflow je možné odhaľovať možné incidenty v sieti, dominantné zdroje prevádzky, sledovanie komunikácie a aké protokoly sa pri komunikácii využívajú.
Prepínače a smerovače, u ktorých je možná podpora Netflow protokolov zaznamenávajú IP prevádzku ktorá prechádza cez dané zariadenie a exportuje tieto dáta do externého zariadenia na ďalšiu analýzu. Netflow architektúra sa obyčajne skladá z niekoľkých Netflow exportérov a jedného kolektora. Exportér je pripojený k monitorovacej linke a analyzuje prechádzajúce pakety. Na základe týchto dát vytvára štatistiky a tie odosiela na Netflow kolektor. Netflow kolektor je databáza na ukladanie štatistických údajov. S touto databázou môžu pracovať rôzne aplikácie, ktoré dokážu nazbierané dáta spracovať do užívateľsky prístupných foriem (graf, tabuľka...).

Netflow architektúry je možné rozdeliť na dve.
Tradičná architektúra je že smerovače a prepínače spracúvajú Netflow štatistiky. Nevýhoda tohto zapojenia je vysoká cena takýchto smerovačov a prepínačom. Tradičná architektúra je zobrazená na obr.9.



Obr.9 zobrazenie Netflow zapojenia tradičnej architektúry

Moderná architektúra oproti tomuto odstraňuje nevýhodu ceny kde sa zaraďuje takzvaná pasívna Netflow sonda. Sú to zariadenia špecializované na monitorovanie a export Netflow štatistík. Výhodou týchto sond je, že je ich možné nasadiť kdekoľvek v sieti. Sondy len monitorujú a nijako nezasahujú do toku paketov – preto pasívne sondy. Potom spracované dáta sú odoslané dedikovanou linkou ku kolektoru. Zapojenie týchto sond je vidno na obrázku.
Podpora Netflow je hlavne u smerovačov a prepínačov spoločnosti Cisco. Kde u smerovačov podpora Netflow je od rady 800, zatiaľ čo u prepínačov podpora tohto protokolu je od modelov rady catalyst 4500.
U voľno dostupných nástrojov pre Netflow je dosť rozšírený NFdump, ktorý funguje z príkazovej riadky. Taktiež je možné doň vkladať vlastné skripty. Na NFdump exituje grafická nadstavba NfSen.
Aby sa mohli získať relevantné dáta z Netflow je potrebný kvalitný analyzátor. Od spoločnosti Cisco sa jedná o CiscoMARS alebo od Fluke netvorks Netflow Tracker.



Obr.10 zobrazenie Netflow zapojenia modernej architektúry

7.3.1 Netflow paket

NetFlow používa veľmi jednoduchý protokol, ktorý funguje cez UDP. Kvôli jednoduchému jednosmernému charakter protokolu, by malo byť relatívne jednoduché pridať mapovanie k iným transportným protokolom ako je napríklad protokol SCTP a TCP.

Hlavička:

0-15	16-31
verzia	počet
čas od štartu(uptime)	
časová známka (timestamp)	
sekvenčné číslo	
zdrojové ID	
dáta	

Tabuľka č.3 hlavička Netflow paketu

Verzia – 16 bitov verzia protokolu
Počet – 16 bitov súčet možností
Čas od štartu – 32 bitov udáva sa v milisekundách a značí čas od naštartovania zariadenia
Časová známka – 32 bitov udáva čas kedy paket opustí zariadenie
Sekvenčné číslo – 32 bitová hodnota. Je to inkrementálny čítač kde pomocou ktorého kolektor kontroluje či v sekvencii paketov poslaných z exportéru nechýbajú pakety.

Zdrojové ID – 32 bitov.

7.3.2 IP tok

Tok IP je základom Newflow protokolu a je definovaný ako tok sekvencie paketov kde majú všetky pakety spoločných päť hodnôt.

1. Zdrojová IP adresa
2. Cieľová IP adresa
3. IP protokol
4. Zdrojový port pre UDP alebo TCP , 0 pre iné protokoly
5. Cieľový port pre UDP alebo TCP , 0 pre iné protokoly

Netflow existuje niekoľko verzií, ale od verzie 5 sa začal masovo používať. Teraz aktuálna je verzia 9. Prenos Netflow záznamov do kolektoru sa deje pomocou protokolu UDP alebo SCTP (Stream Control Transmission Protokol). Po prenose je daný záznam exportéra zahodený. To je dôvod prečo je možné stratiť tieto dáta ak pri prenose nastala chyba.
Netflow verzie 5 obsahuje tieto položky:

- Číslo verzie
- Sekvenční číslo
- SNMP index vstupného a výstupného rozhraní (umožňuje sledovať vyťaženie jednotlivých sieťových rozhraní, vyžaduje zoznam rozhraní prístupný pomocou SNMP)
- Čas začiatku a konce IP toku (tzn. výskyt prvého a posledného paketu tohto toku)
- Počet bajtov a paketov v toku
- Údaje z L3 hlavičky:
    - Zdrojové a cieľové IP adresy
    - Zdrojové a cieľové porty
    - IP protokol
    - Type of Service (ToS)
- U TCP tokov obsahuje množinu tvorenou zjednoteným všetkých TCP flagov, ktoré sa v toku vyskytli.
- Smerovacie informácie:
    - IP adresa ďalšieho skoku (dôležité pre analýzu smerovacícj postupov)
    - Maska cieľovej a zdrojové IP adresy (dĺžky prefixov podľa CIDR notácie)

7.4 Syslog

Pôvodný Syslog vznikol v roku 1980 ako súčasť projektu Sendmail a potom bol štandardizovaný IETF. Syslog je štandard na preposielanie správ z logov po sieti. Slúži k tomu aby sme koncentrovali logy z rôznych zariadení a aplikácií na jedno miesto a mohli sme na tieto správy adekvátne reagovať. Tento štandard funguje na princípe klient – server. Na strane klienta je potrebná aplikácia, ktorá odosiela správy z logu pomocou protokolu Syslog. Ďalej je potrebný Syslog server, ktorý tieto správy

spracováva. Syslog správy používajú k transportu UDP protokol a sú prijímané na porte 514. Syslog správa býva obyčajne nie väčšia ako 1024 bytov.

7.4.1 Formát syslog paketu.

Paket sa skladá z troch častí. PRI, hlavičky a MSG. PRI je skratka od Priority (priorita). Je to číslo uzatvorené v hranatých zátvorkách. Je to osembitové číslo. Prvé tri znaky reprezentujú závažnosť správy. Tri bity dávajú osem stupňov.

číslený kód	závažnosť
0	systém je nepoužiteľný
1	hneď musia byť vykonané kroky
2	kritické podmienky
3	chybová podmienka
4	výstražná podmienka
5	normálna ale vážna podmienka
6	informačná správa
7	debugovacia správa

Tabuľka č.4 PRI význam znakov

Ďalších 5 bitov udáva typ aplikácie ktorá vyvolala správu.

číslený kód	závažnosť
0	kernel messages
1	user-level messages
2	mail system
3	system deamons
4	security/authorization messages
5	messages generated intrnaly by syslog
6	line printer
7	network news susbystem
8	UUCP subsystem
9	clock deamon
10	security/authorization messages
11	FTP deanom
12	NTP subsystem
13	log audit
14	log alert
15	cock deamon
16	local use 0
17	local use 1
18	local use 2
19	local use 3
20	local use 4
21	local use 5
22	local use 6
23	local use 7

Tabuľka č.5 typ apolikácie

Hlavička obsahuje:

- Časovú značku. Tu je zaznačený čas vytvorenia správy. Treba si pamätať, že ak je systémový čas na zariadení nastavený zle tak aj v hlavičke tento čas bude zlý.
- Meno hosťa s jeho IP adresou.

MSG

Táto časť vyplní zvyšok paketu. Toto obsahuje ďalšie informácie o vytvorení správy. MSG časť má dve polia:

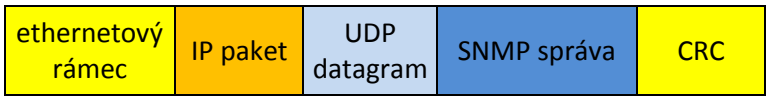
- Pole tag
- Obsah poľa

Hodnota v poli TAG bude názov programu alebo procesu, ktorý vygeneroval správu. OBSAH obsahuje podrobné informácie o správe.

Okolo tohto protokolu sa vytvoril rad implementácií a z nich jedna sa volá syslog-ng. Keďže na sieti býva značná prevádzka a zápisov v logoch je veľké množstvo Syslog umožňuje vytvoriť skripty, ktoré analyzujú prichádzajúce správy a upozornia nás na problémy.

7.5 SNMP (Simple Network Management Protocol)

SNMP je jednoduchý protokol umožňujúci monitorovanie a správu v sieti. SNMP je časť protokolovej sady TCP/IP. Operuje na siedmej vrstve OSI modelu a používa pre transport protokol UDP na portoch 161 a 162.



Obr.10

Architektúra SNMP rozpoznáva minimálne dva komponenty:
- spravovaný objekt
- spravovacia stanica

SNMP datagram sa skladá z hlavičky ktorá obsahuje verziu SNMP protokolu, identifikačné číslo datagramu (pre priradenie odpovede), informáciu o chybe (nastavenú v SNMP Response datagrame), autentifikačnú informáciu a typ PDU (SNMP Get Request, SNMP Get Response a pod). PDU (Protocol Data Unit) obsahuje zoznam OID ktoré identifikujú čítané alebo nastavované premenné a tiež ich hodnoty (v prípade SNMP Get datagramov prázdnu hodnotu - ASN NULL).
SNMP využíva dva hlavné typy komunikácie. Jeden typ je smerom od manažéra k agentovi. Napríklad ak manažér potrebuje zistiť aktuálne informácie o zariadení. Hodnoty datagramu na dotaz na odpoveď sú zobrazené na obr.11.

vezia	community string	PDU typ	ID dotazu	error status	error ID	OID	hodnota

Obr.11 hodnoty datagramu dotazu na odpobeď

Druhý typ správ sú takzvané trapy kedy agent vysiela správu nie na výzvu od manažéra, od udalosti, ktorá sa vyskytla v sieti a agent má zadané, že pri tejto konkrétnej udalosti odošle správu. Hodnoty v datagrame na dotazy trap sú zobrazené na obrázku 12.

Dotaz pre trapy

vezia	community string	PDU typ	enterprise	agent IP	gen trap	spec trap	čas	objekt 1 hodnota 1	...

Obr.12 hodnoty datagramu dotazu na trapy

Verzie protokolu SNMP

- SNMPv1 - Prvá verzia SNMP protokolu bola definovaná v roku 1988 (RFC 1065-1067). Autentifikácia klienta (spravovaného) bola riešená pomocou tzv. „community string“, ktorý bol prenášaný ako čistý reťazec. Najmä preto sa protokol ďalej vyvíjal.
- SNMPv2 - Verzia 2 sa snažila odstrániť nedostatky SNMPv1. Vzniklo mnoho jej odnoží ktoré riešili bezpečnosť a rozšírenia protokolu. Nakoniec sa stala prakticky štandardom SNMP v2, ale autentifikácia ostala na úrovni SNMPv1.
- SNMPv3 - Verzia SNMPv3 tak konečne štandardizovala nové autentifikačné mechanizmy

7.6 ICMP (Internet control Message Protocol)

Internet Control Message Prtocol je obslužný protokol pre TCP/IP, ktorý poskytuje informácie o dostupnosti zariadenia, služieb alebo tras v sieti TCP/IP. Väčšina metód a nástrojov na riešenie problémov vsieti je založený na bežných typoch správ protokolu ICMP. Protokol ICMP je definovaný v dokumentu RFC 792.

7.6.1 Hlavička ICMP

Protokol ICMP je podmnožinou protokolu IP a pri prenose správ spolieha na protokol IP. ICMP používa hlavičku, ktorej veľkosť sa mení v závislosti na účelu správ. Na obrázku XX
je zobrazená hlavička ICMP.

Protokol ICMP			
bitový posun	0 - 15		16 -31
0	Type	Code	Checksum
32	Variable		

Obr.13 hlavička ICMP

Type (Typ) – typ alebo klasifikácia správy ICMP
Code (Cód) – čiastkové klasifikácie správy ICMP
Checkosum (Kontrolný súčet) – po doručení paketu overuje, či neprišlo k narušeniu obsahu hlavičky ani dát.
Variable (Premenná) – časť, ktorá je závislá na poliach Type a Code.

7.6.2 Aplikácia Ping

Ping je jednoduchý testovací mechanizmus vytvorený na testovanie dostupnosti uzla. Ide o kombináciu správ protokolu ICMP typu 0 a 8, tzv. Echo Request a Echo Reply. Tento program odošle sériu paketov na cieľovú adresu a čaká na spätnú odpoveď.
Niektoré nastavenie programu Ping:

- ping –t ..... robí test v cyklu pokiaľ nie je prerušený
- ping –a ..... urobí prepis adresy na meno
- ping –n počet ..... urobí príslušný počet pokusov o odpoveď
- ping –l veľkosť ..... veľkosť vyrovnávajúcej pamäte k odoslaní
- ping –f ..... nastavuje príznak nefragmentovať (don´t fragment)
- ping –i TTL ..... nastavuje TTL (Time To Live - maximálný počet priechodov cez smerovač)
- ping –w timeout ..... zaisťuje predĺženie doby vypršania čakania na odpoveď (timeout); parametrom je číslo v milisekundách

Príklad výpisu oneskorenia pomocou programu ping:

```
C:\>ping cs.wikipedia.org

Příkaz PING na rr.knams.wikimedia.org [91.198.174.2] s délkou 32
bajtů:

Odpověď od 91.198.174.2: bajty=32 čas=19ms TTL=60
Odpověď od 91.198.174.2: bajty=32 čas=19ms TTL=60
Odpověď od 91.198.174.2: bajty=32 čas=19ms TTL=60
Odpověď od 91.198.174.2: bajty=32 čas=19ms TTL=60

Statistika ping pro 91.198.174.2:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 19ms, Maximum = 19ms, Průměr = 19ms
```

Na konci výpisu sú zhrnuté všetky informácie ako sú stratené pakety, minimálna latencia, maximálna latencia a priemer.

7.6.3 Aplikácia Tracert

Je to aplikácia na zisťovanie cesty kadiaľ sa k zadanému cieľu dostanem, čiže cez ktoré uzly v sieti prechádza komunikácia. Vďaka získaným informáciám je možné zistiť problémové miesta v sieti, ktoré spomaľujú komunikáciu v sieti. Aplikácia pracuje s parametrom TTL (Time To Live). Testovacie pakety sa odošlú z určitou hodnotou TTL a každým minutým uzlom sa táto hodnota zníži až kým nedorazí z cieľovému uzlu (pokiaľ má nastavenú dostatočne veľkú hodnotu TTL) alebo keď

hodnota TTL je rovná nule daný uzol, ktorý nie je cieľový odošle ICMP správu time exceeded.
Niektoré nastaviteľné parametre programu tracert:

- -h maximum_hops ….. max. počet preskokov (hops) k dosiahnutia cieľa
- -w timeout ….. zaisťuje predĺženiedoby vypršaniaí čakania na odpoveď z každého uzlu (timeout); parametrom je číslo v milisekundách
- -j host-list ….. smerovánie podľa zoznamov uzlov v ceste (source routing)

7.6.4 Aplikácia Pathping

Táto aplikácia kombinuje funkcie príkazov ping a tracert. Určitú dobu opakovane zasiela všetkým smerovačom medzi zdrojom a cieľom správy s požiadavkou na odozvu a na základe vracajúcich paketov od jednotlivých smerovačov získava výsledky. Keďže pathping zobrazuje úroveň straty paketov na všetkých uzloch môže určiť kde v sieti vznikajú problémy .

7.7 Paketové sniffery

Analýza paketov, ktorá sa označuje ako aj sledovanie paketov (packet sniffing) alebo analýza protokolov, popisuje proces zachytávania a interpretácie aktuálnych dát prenášaných po sieti. Vďaka tomu je možné porozumieť fungovaniu siete. K analýze paketov sa obyčajne používa paketový sniffer, ktorý umožňuje zachytávať neformátované dáta pri prenose.
Analýza paketov poskytuje nasledujúce možnosti:

- Zoznámením sa s vlastnosťami siete
- Zistenie užívateľov siete
- Zistenie, kto alebo čo spotrebúva šírku pásma
- Identifikácia časov špičkového využitia siete
- Identifikácia možných útokov alebo škodlivé aktivity
- Vyhľadávanie nezabezpečených a neefektívnych aplikácií

Predpokladom efektívnej analýzy paketov je rozhodnutie o tom, kam umiestniť paketový sniffer, tak aby bol najúčinnejší. Problém zapojenia snifferu je v tom, že k prepojení zariadení používa veľa zariadení(prepínače, smerovače, rozbočovače). Tieto prepojovacie zariadenia sa vzájomne líšia v tom aké informácie sú získané pomocou snifferu keď je umiestnený v rôznych častiach siete. Preto je dôležité poznať fyzické rozloženie siete na to, aby boli získané požadované dáta.
Sledovanie paketov vyžaduje sieťovú kartu, ktorá umožňuje prechod do promiskuitného režimu. Vďaka tomu môže sieťová karta sledovať pakety prechádzajúce sieťou.
Sledovanie paketov na rozbočovači.
Ak sa chce sledovať prevádzku na rozbočovači, stačí ak sa paketový sniffer pripojí k voľnému portu rozbočovača. Môže sa tak sledovať kompletná prichádzajúca

a odchádzajúca komunikácia všetkých zariadení, ktoré sú pripojené k danému rozbočovaču.

7.7.1 Sledovanie prevádzky na prepínačoch.

Ak sa pripojí sniffer k prepínaču je možné sledovať len broadcastovú a svoju vlastnú prevádzku. Ak je potrebné zachytávať prevádzku z cieľového zariadenia v prepínanej sieti je možné použiť jednu zo štyroch hlavných metód.

- Zrkadlenie portu
- Rozbočovanie
- Použitie odposluchu
- Znehodnotenie medzipamäte ARP

Zrkadlenie portu

Tento spôsob predstavuje asi najjednoduchší spôsob ako zachytávať komunikáciu na cieľovom zariadení v prepínanej sieti. Pri tejto možnosti je nutné aby daný prepínač podporoval zrkadlenie portov. Potom je len potrebné zadať príkaz prepínaču aby kopíroval všetku prevádzku daného portu na nami zvolený port. Niektorí výrobcovia prepínačov umožňujú zrkadliť viacero portov na jeden.

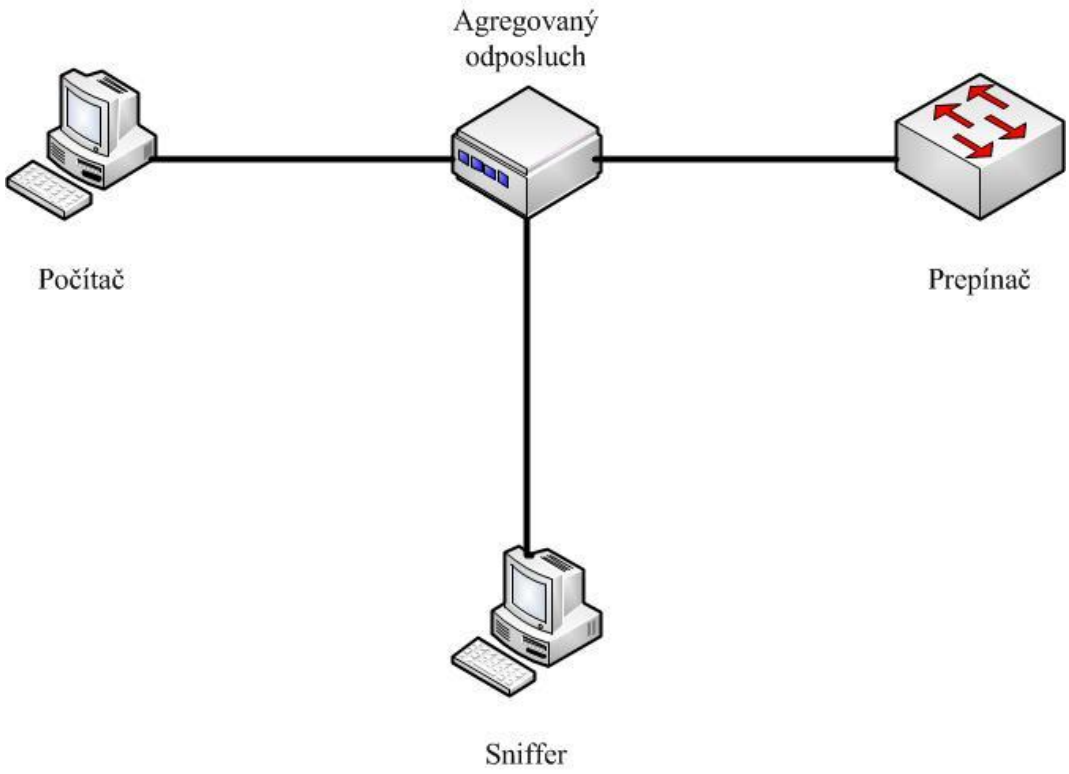
Rozbočovanie

Tento postup je založený na umiestnení cieľového zariadenia a analyzátora do rovnakého sieťového segmentu. To sa docieli tak, že obidve zariadenia sa pripoja priamo do rozbočovača.

Použitie odpočúvania

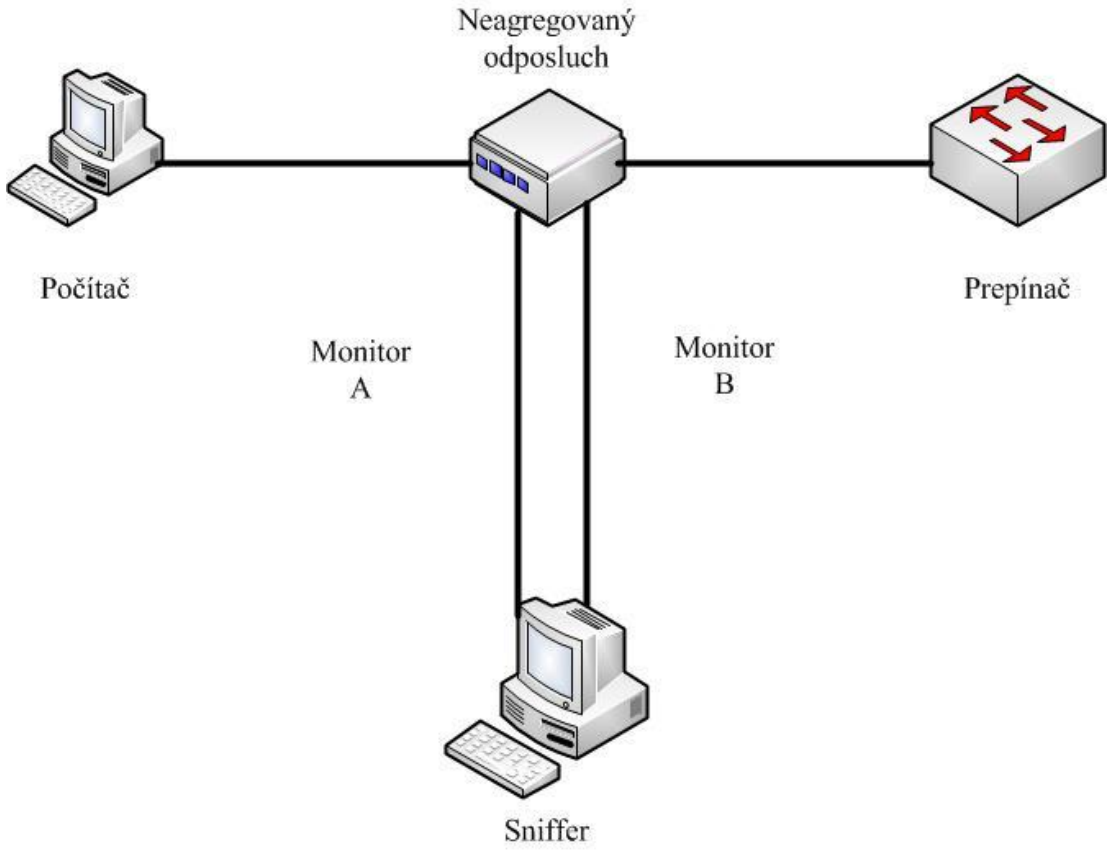
Sieťové odpočúvanie je zariadenie, ktoré je možné umiestniť medzi dva body v kabeláži ak je vyžadované zachytávať pakety medzi nimi. K dispozícii sú dva typy sieťových odpočúvaní a to.

Agregované odpočúvanie má len tri porty a inštalácia je jednoduchšia. Jeden z troch portov je určený k sledovaniu obojsmernej komunikácie.



Obr.14 zobrazenie agregovaného odpočúvania

Neagregované odpočúvanie má štyri porty a miesto jedného odpočúvacieho portu má dva. Jeden odpočúvací port slúži na sledovanie v jednom smere a druhý port v tom druhom smere.



Obr.15 zobrazenie neagregovaného odpočúvania

Znehodnotenie medzipamäti ARP

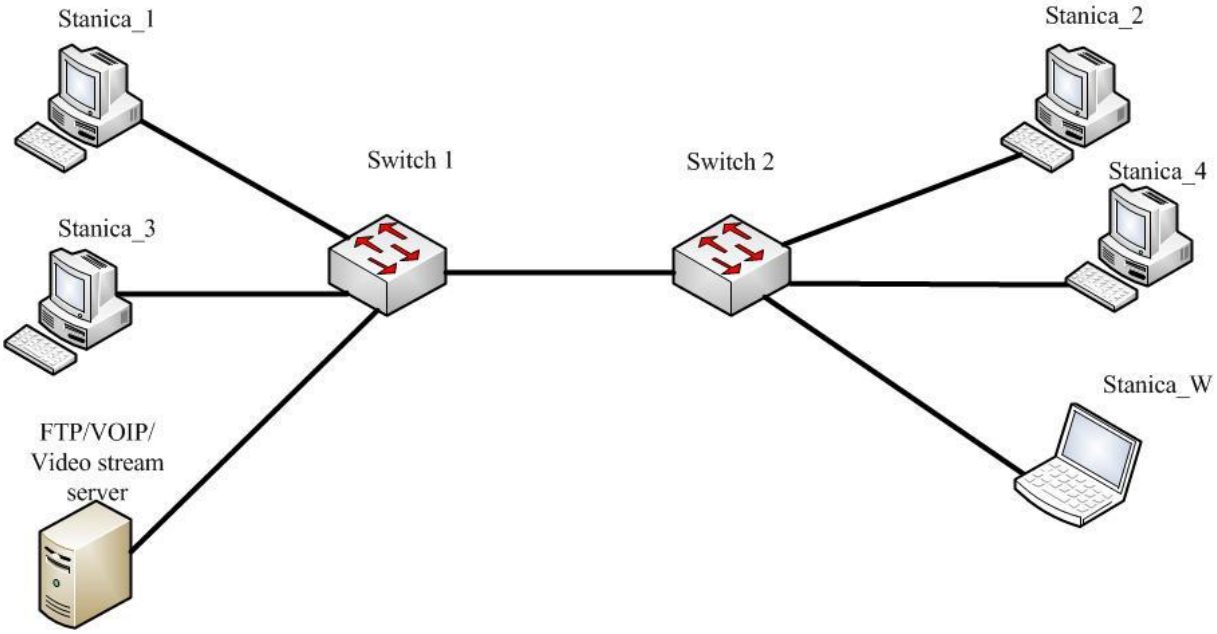
Znehodnotenie medzipamäti ARP alebo nazývané ako falšovanie ARP je založené na odosielaní špeciálnych správ ARP ethernetovému prepínaču alebo smerovaču. Tieto správy majú pritom podvrhnutú MAC adresu, aby bolo možné zachytávať prevádzku iného počítača.

7.7.2 Sledovanie prevádzky v smerovanom prostredí

Všetky metódy na odpočúvanie linky v sieti s prepínačmi sú dostupné aj v sieti so smerovačmi. V smerovanom prostredí je potrebné brať ohľad na umiestnenie snifferu, ktoré je obzvlášť dôležité pri riešení týkajúcich sa viacerých sieťových segmentov. V prípadoch kedy dáta prechádzajú cez viacero smerovačov, je dôležité analyzovať prevádzku na obidvoch stranách smerovača.

8 Praktická časť

Cieľom praktickej časti diplomovej práce je meranie parametrov dátových sietí. Tieto parametre sú analyzované pomocou paketového sniffera.



Obr.16 zobrazenie praktického merania parametrov siete

Server	192.168.1.100
Switch_1	192.168.1.1
Switch_2	192.168.1.2
Stanica_1	192.168.1.11
Stanica_2	192.168.1.67
Stanica_3	192.168.1.10
Stanica_4	192.168.1.12
Stanica_W	192.168.1.200

Tabuľka č.3 IP adresy zariadení

Obrázok jednoducho znázorňuje prepojenie staníc. Zariadenia sú v jednej logickej sieti na lepší dohľad. Testovaciu sieť som vytvoril pomocou dvoch aktívnych smerovačov
Použité zariadenia
Na vytvorenie testovacej siete boli využité zariadenia podniku NSP Skalica a.s.

Zyxel GS1510-24 – je konštruovaný pre konektivitu typu plug-and-play a jednoducho sa inštaluje. Zariadenie sa ovláda cez SNMP (Simple Network Management Protocol) a webové grafické rozhranie. Ovládanie prepínača je rozdelené na dva režimy, tzv. „inteligentný režim“ a „pokročilý režim“. Prepínač obsahuje dva otvorené Gigabit SFP sloty. Podporuje maximálnu teoretickú rýchlosť štandardnej kabeláže CAT-5 podľa štandardov IEEE(manual www).

Samotné pracovné stanice boli potom PC s parametrami, ktoré sú uvedené v tabuľke.

FTP/VoIP/Video server	intel Core i3 4GB RAM	MS Windows 7 Profesional SP1
Stanica_1	Intel Celeron 1GB RAM	MS Window XP Profesional SP3
Stanica_2	intel Core 2 duo 4GB RAM	MS Windows wista Home premium
Stanica_3	intel Celeron 2GM RAM	MS Windows XP Home SP3
Stanica_4	intel Celeron 2GM RAM	MS Windows 7 Home Premium SP1
Wireshark monitor	intel Core i3 4GB RAM	MS Windows 7 Home premium SP1

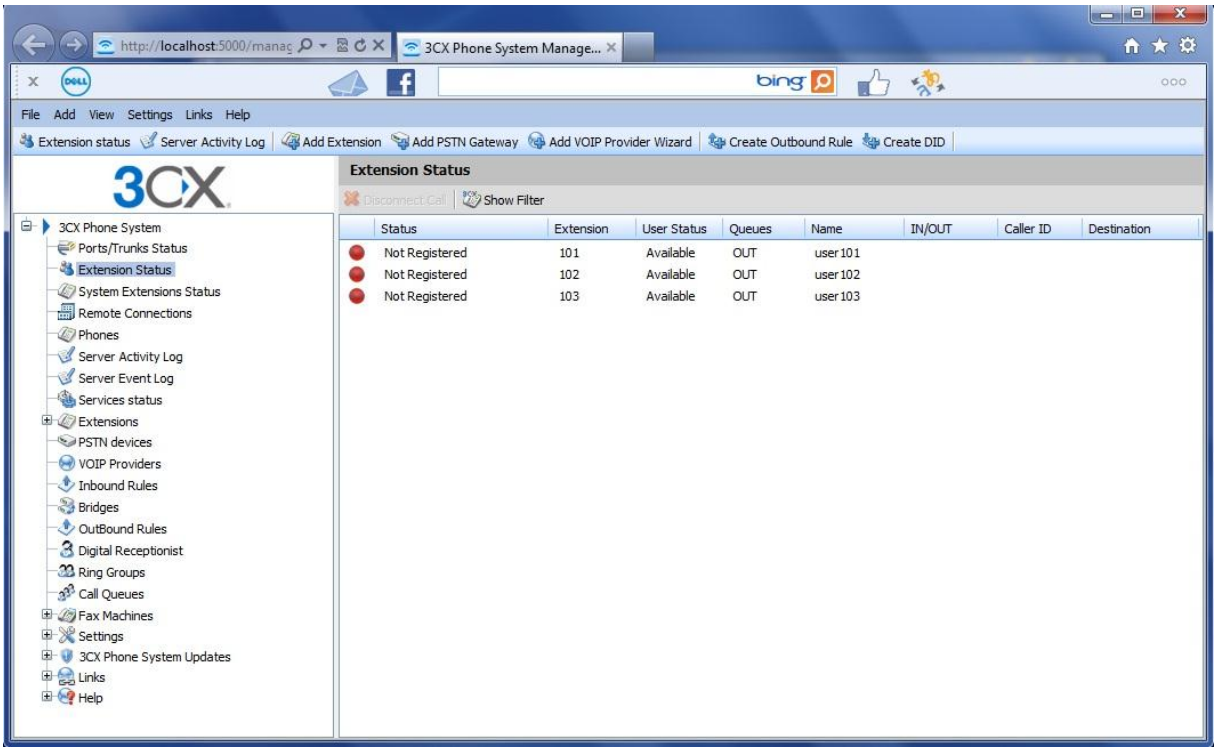
Tabuľka č.4 parametre použitých zariadení

Názov programu	Verzia programu
VLC media player	1.11.1
3CX Phone System	10.0.24018.2322
3CX Phone	6.0.20943.0
GuildFTPd	0.999.13
Abyss web server X1	2.7
Wiresark	1.6.7
UltraVNC	1.0.56

Tabuľka č.5 použitý softvér

Vzhľadom na nemožnosť využiť reálne IP telefóny boa zvolený softwarový variant.

Pre VoIP komunikáciu boli zvolené produkty od spoločnosti 3CX. Táto spoločnosť na svojich internetových stránkach http://www.3cx.com/ poskytuje možnosť stiahnuť si pobočkovú ústredňu 3CX Phone System a softwarový telefón 3CX Phone. Ústredňa 3CX vyžaduje aby bol na serveri nainštalovaný a spustený web server. K tomuto účelu bol použitý Abyss web server X1.
Po jednoduchej inštalácii pobočkovej ústredne stačilo pre potreby úlohy nakonfigurovať IP adresu servera kde je nainštalovaná ústredňa. Potom boli vytvorené jednotlivé účty 101, 102, 103. Neplatená verzia tejto ústredne podporuje tri súčasne prebiehajúce hovory. Ostatné parametre a možnosti neboli pre potreby navrhnutej úlohy využité. Ďalšie možnosti ústredne sú: nastavenie odkazovača pri nedostupnosti volaného, možnosť volania interné linky atď. Prípadné zmeny nastavenia ústredne je možné upravovať cez webové konfiguračné rozhranie.



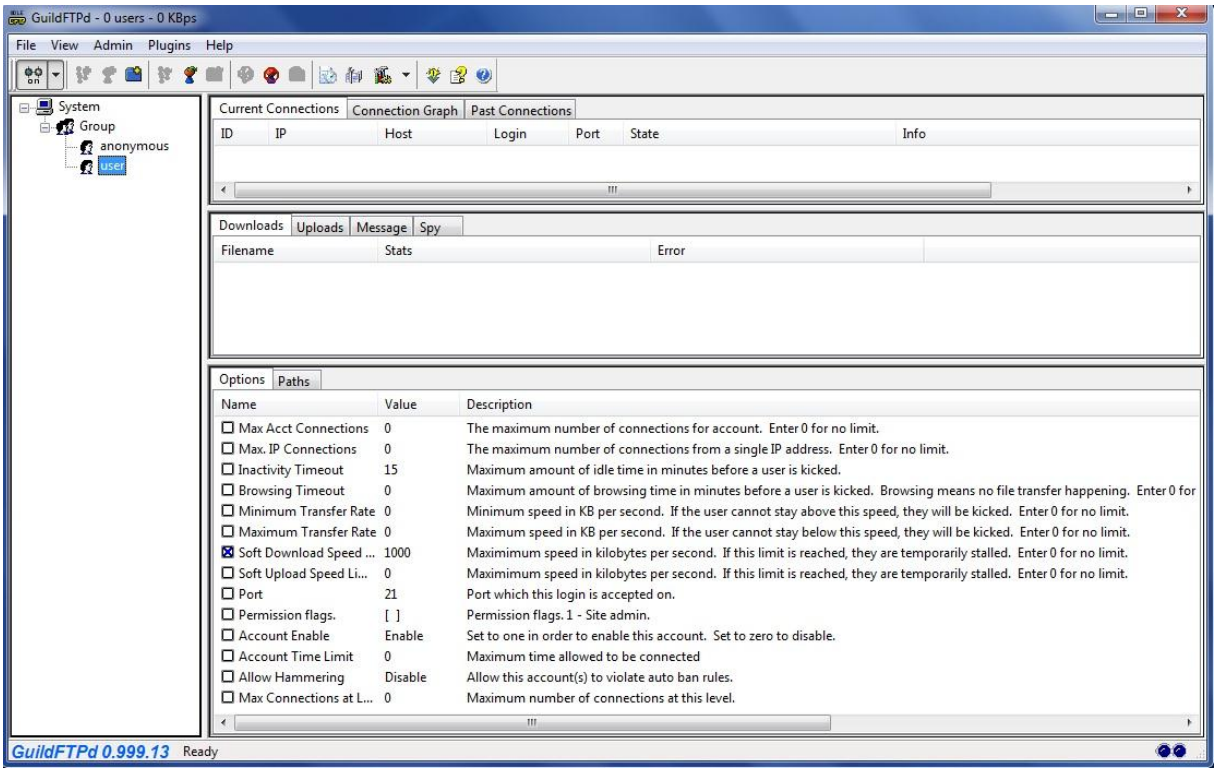
Obr.17 konfiguračné rozhranie ústredne 3CX

Podobne ako u telefónnej ústredne tak aj u softwarového telefónu je inštalácia jednoduchá. Po inštalácii je len potrebné zaregistrovať užívateľa.

Obr.18 softvérový telefón 3CX

Pre stream videa bol zvolený program VLC media player. V prílohe je popísaný návod na vytvorenie streamovaného videa.

Ako FTP server bola zvolená voľne dostupná aplikácia GuildFTPd (http://www.slunecnice.cz/sw/guildftpd/). Dôvod k vybratiu tohto FTP servera je jeho jednoduchá konfigurácia, ktorá sa robí cez grafické rozhranie.



Obr.19 konfiguračné rozhranie FTP servera

Pri otvorení nastavenia servera je možné ľahko pridávať nových užívateľov a meniť nastavenia jednotlivých užívateľov. Samotný FTP server dokáže zaznamenávať prevádzku na FTP serveri.

FTP účty		
Názov	Heslo	Max. prenosová rýchlosť
user1	user1	1000 kB/s
user2	user2	neobmedzená

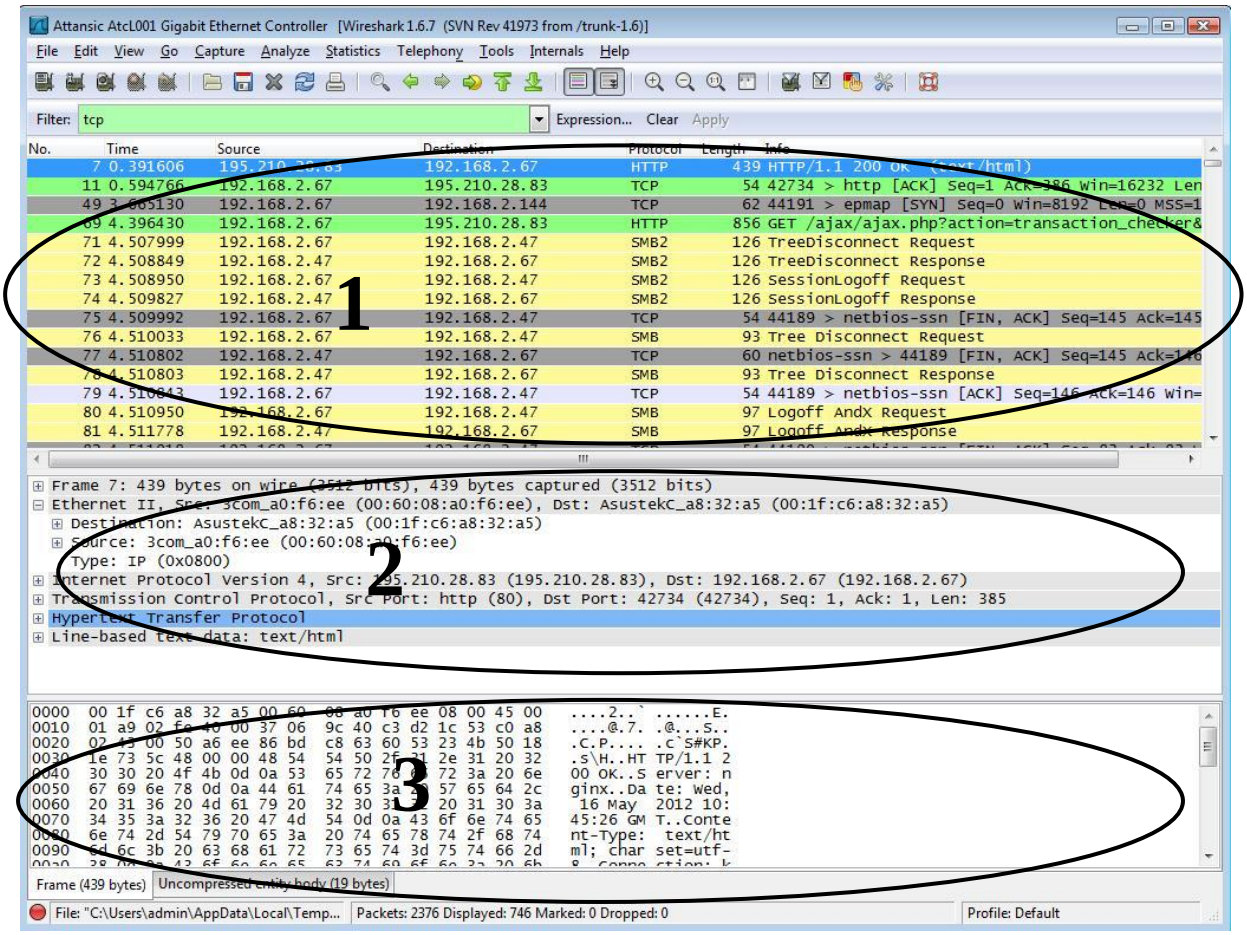
Tabuľka č.6 nastavenie FTP účtov

Na vzdialenú komunikáciu medzi stanicami bol použitý program UltraVNC.

8.1 Program Wireshark

Hlavné okno programu je rozdelené na tri časti. Packet List – horné podokno obsahujúce tabuľku so všetkými zachytenými paketmi a aktuálnom zachytenom súbore. V jednotlivých stĺpcoch sú uvedené čísla paketov, relatívne časy, ich zachytenia, ich zdroj, cieľ, príslušné protokoly a niektoré všeobecné informácie. Packet Details – stredné podokno hierarchicky zobrazuje informácie o jedinom vybranom pakete. Packet Bytes – dolné podokno ukazuje obsah paketu v jeho nespracovanej podobe. Zobrazuje tak paket ako vyzerá pri prenose po sieti.

Tieto tri časti na sebe závisia. Ak je potrebné zobraziť podrobnosti o jednotlivom pakete v okne Packet Details jednoducho sa kline na požadovaný paket v okne Paket List. Po výbere paketu je možné kliknutím v podokne Packet Details vybrať jeho časť a s podokne Packet Bytes sa zobrazia zodpovedajúce bajty.



Obr.20 hlavné okno programu Wireshark

Pre lepšiu orientáciu je v programe možnosť farebne kódovať v podokne Packet List jednotlivé protokoly. Napríklad prevádzka protokolu DNS je značená modrou farbou a protokol http je značený zelenou farbou. Pre zistenie ktorá farba prislúcha danému protokolu slúži menu Coloring Rules.

Filtre umožňujú presne určiť, ktoré pakety budú k dispozícii pre analýzu. Wireshark má už implicitne nastavené niektoré typy filtrov, no je možné si aj nadefinovať vlastné filtre. Syntax vytvárania filtrov prístupný na internetových stránkach programu Wireshark (http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html)

Filtre programu Wireshark sa delia na dva typy:

- Filtre zachytávajúce (capture filter) sa nastavujú pri zachytávaní paketov a zaistia len tie pakety, ktoré sú udané v podmienkach.
- Filtre zobrazenia (display filter) sa aplikujú na už zachytené pakety kedy je možné zobraziť len tie pakety, ktoré zodpovedajú zadaným parametrom.

Príklady rôznych filtrov:

ip.addr == 10.0.0.1 nastaví filter na zobrazenie paketov s adresou 10.0.0.1]

http or dns [nastaví filter na zobrazenie http a dns]

tcp.flags.reset==1 [zobrazí všetky TCP segmenty s príznakom reset]

udp contains 33:27:58 [nastaví filter na hexadecimálne hodnoty 0x33 0x27 0x58]

http.request [zobrazí HTTP GET request]

Na zisťovanie parametrov siete je hlavnom okne programu záložka Statistics a zvlášť pre IP telefóniu záložka Telephony. Tieto záložky poskytujú množstvo možností pre analýzu prenosu.

8.2 Nastavenie prepínačov

Prepínače sa nastavujú po pripojení k zariadeniu pomocou internetového prehliadača. Nastavenie v tomto režime intuitívne a prehľadné. Maska siete sa nastavila na 255.255.255.0. Rýchlosť na portoch bola nastavená na 100Mb/s - full duplex a nastavené zrkadlenie portov na jeden port kde je pripojená stanica s paketovým snifferom. Port, na ktorom bolo nastavenie zrkadlenie portov a pripojená stanica Stanica_w bola nastavená na 1Gb/s - full duplex.

8.3 Výsledky merania

Po spustení staníc sa na Stanici_w spustil program Wireshark. Bolo spustené streamovanie videa. Potom bolo pomocou programu UltraVNC pripojené na stanice s označením Stanica_1, Stanica_3, Server kde sa postupne zahájili telefónne rozhovory s medzi stanicami Stanica_2 -> Stanica_1 a Stanica_3 -> Stanica_4. Ďalej bol spustený príjem videa na stanici pomocou VLC media player na stanici s názvom Stanica_2 a spustil príjem súboru pomocou FTP protokolu zo servera stanicami Stanica_2 a Stanica_4.
Po skončení prenosu FTP na obidvoch staniciach sa postupne ukončilá všetka komunikácia a celá komunikácia v programe Wireshark sa uložila pod názvom *komunikácia.pcap*.

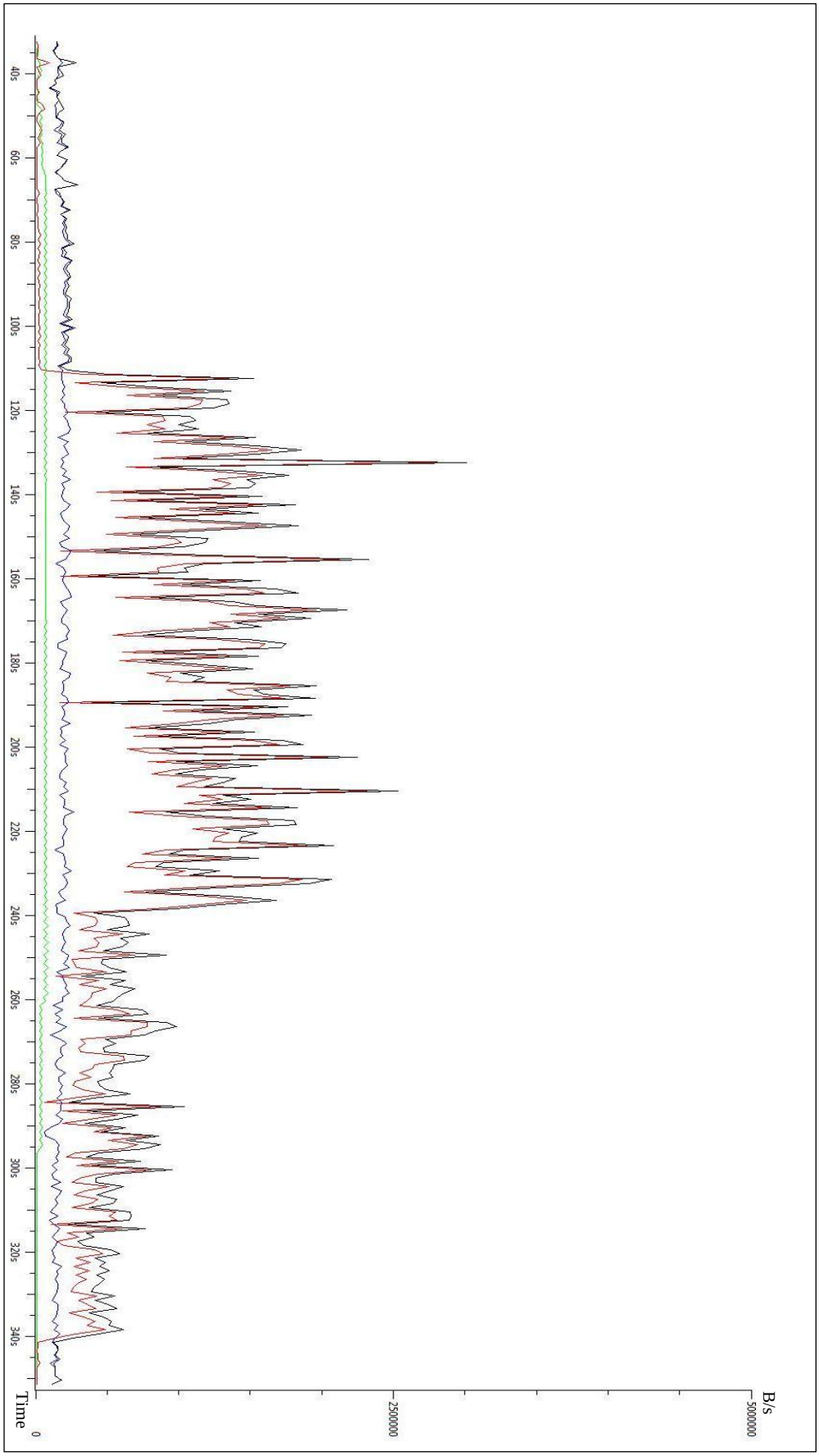
8.3.1 Priemerné rýchlosti jednotlivých spojov

Priemerné rýchlosti jednotlivých spojov je možné získať ak do filtra sú postupne zadané tieto hodnoty:
ip.addr == 192.168.1.100 && ip.addr == 192.168.1.67
ip.addr == 192.168.1.100 && ip.addr == 192.168.1.12
ip.addr == 192.168.1.10 && ip.addr == 192.168.1.12
ip.addr == 192.168.1.11 && ip.addr == 192.168.1.67
Za každým v menu Statistics → Summary sú spočítané hodnoty pre vybrané pakety zodpovedajúce filtru.

Komunikácia	Rýchlosť	Prenesené dáta
100 ↔ 67	350,668 kB/s	117,184 MB
100 ↔ 12	179,696 kB/s	61,714 MB
10 ↔ 12	32,18kB/s	7,687 MB
11 ↔ 67	28,67kB/s	9,721 MB

Tabuľka č.7 rýchlostí a prenesených dát jednotlivými spojmi

Ako je vidno z grafu č.2 umiestneného ako na konci práce najväčšie zastúpenie prevádzky má TCP protokol.



Graf č.2 čierna celková prevádzka, červená prevádzka TCP, zelená prevádzka RTP, modrá prevádzka UDP

8.3.2 TCP rýchlosť

Rýchlosť prenosu pri TCP spojení zistíme v programe nasledovne Statistics → Conversation list → TCP(IPv4 & IPv6)

TCP Conversations: 12

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
192.168.1.67	59980	192.168.1.100	49300	113 357	117 154 830	36 721	2 349 202	76 636	114 805 628	111.405106000	126.8866	148113.50	7238314.74
192.168.1.100	49304	192.168.1.12	49182	64 655	61 693 531	40 002	60 100 337	24 653	1 593 194	162.383407000	178.0325	2700645.01	71591.14
192.168.1.67	59975	192.168.1.10	rfb	7 961	3 143 072	3 531	215 645	4 430	2 927 427	18.413782000	332.4499	5189.23	70444.95
192.168.1.67	59974	192.168.1.11	rfb	7 140	2 719 378	3 103	189 135	4 037	2 530 243	10.676440000	339.0408	4462.83	59703.57
192.168.1.67	59979	192.168.1.100	49299	9	868	4	246	5	622	104.896156000	0.3036	6483.07	16392.15
192.168.1.100	49303	192.168.1.12	49181	9	868	5	622	4	246	154.301029000	3.0015	1657.83	655.67
192.168.1.67	59978	192.168.1.100	ftp	41	3 077	22	1 398	19	1 679	83.705599000	154.9837	72.16	86.67
192.168.1.12	49180	192.168.1.100	ftp	38	2 850	20	1 274	18	1 576	137.162784000	203.5371	50.07	61.94
192.168.1.11	neod2	192.168.1.67	netbios-ssn	8	480	4	240	4	240	77.022921000	255.7647	7.51	7.51
192.168.1.10	neod2	192.168.1.67	netbios-ssn	8	480	4	240	4	240	21.072016000	320.0359	6.00	6.00
192.168.1.67	59981	192.168.1.11	epmap	3	194	3	194	0	0	265.297243000	8.9885	172.66	N/A
192.168.1.67	59982	192.168.1.11	epmap	3	194	3	194	0	0	286.590303000	8.9923	172.59	N/A

Tabuľka č.8 zoznam TCP spojení

V tabuľke číslo 8 sú zobrazené všetky TCP spojenia. Prvé dva riadky zobrazujú mnou vytvorený prenos dát z FTP servera. Rýchlosť je udávaná v bitoch za sekundu. Po prepočítaní sú hodnoty zobrazené v tabuľke.

cieľová adresa	rýchlosť [kB/s]
192.168.1.67	904,78
192.168.1.12	337,58

Tabuľka č.9 namerané rýchlosti FTP prenosu

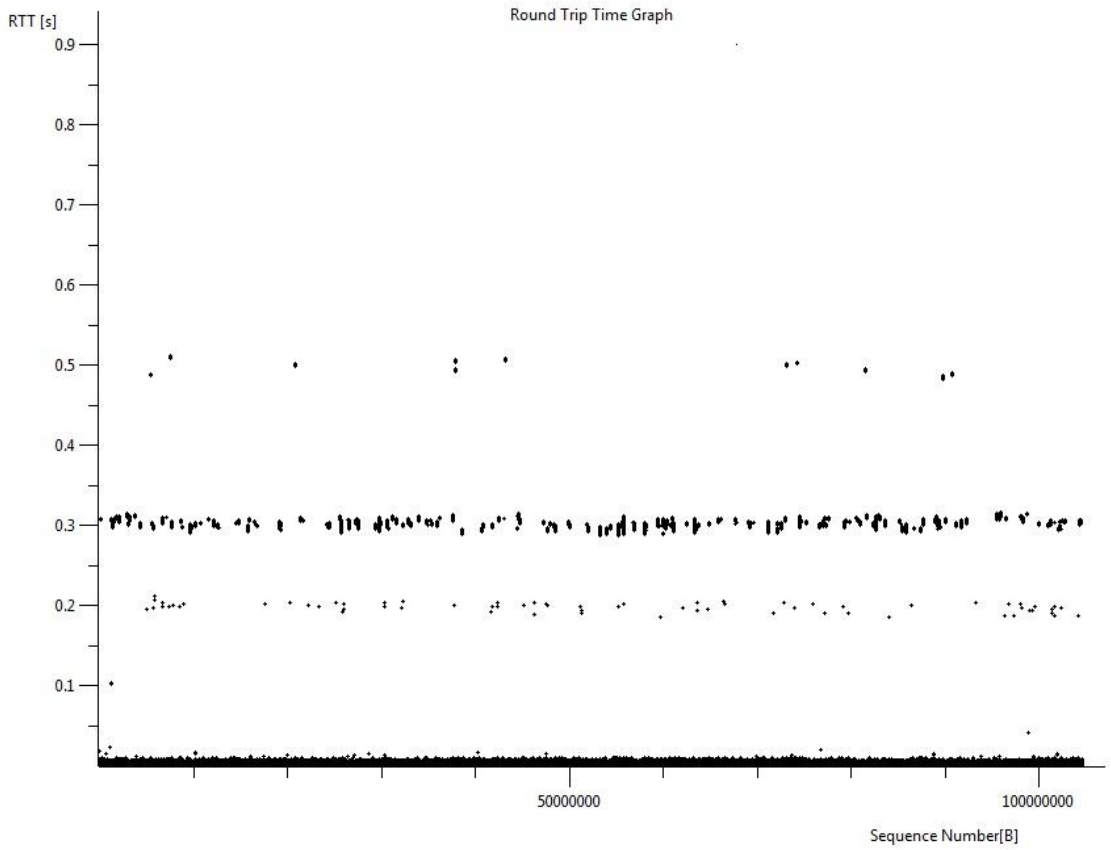
Keďže pri prenose súboru na cieľovú adresu 192.168.1.12 bol pri prihlásení na FTP server využitý účet s neobmedzenou hodnotou sťahovania bola zistená chyba na káblovom prepojení so stanicou s názvom Stanica_4 a prepínačom Switch_2.

8.3.3 Stratovosť TCP

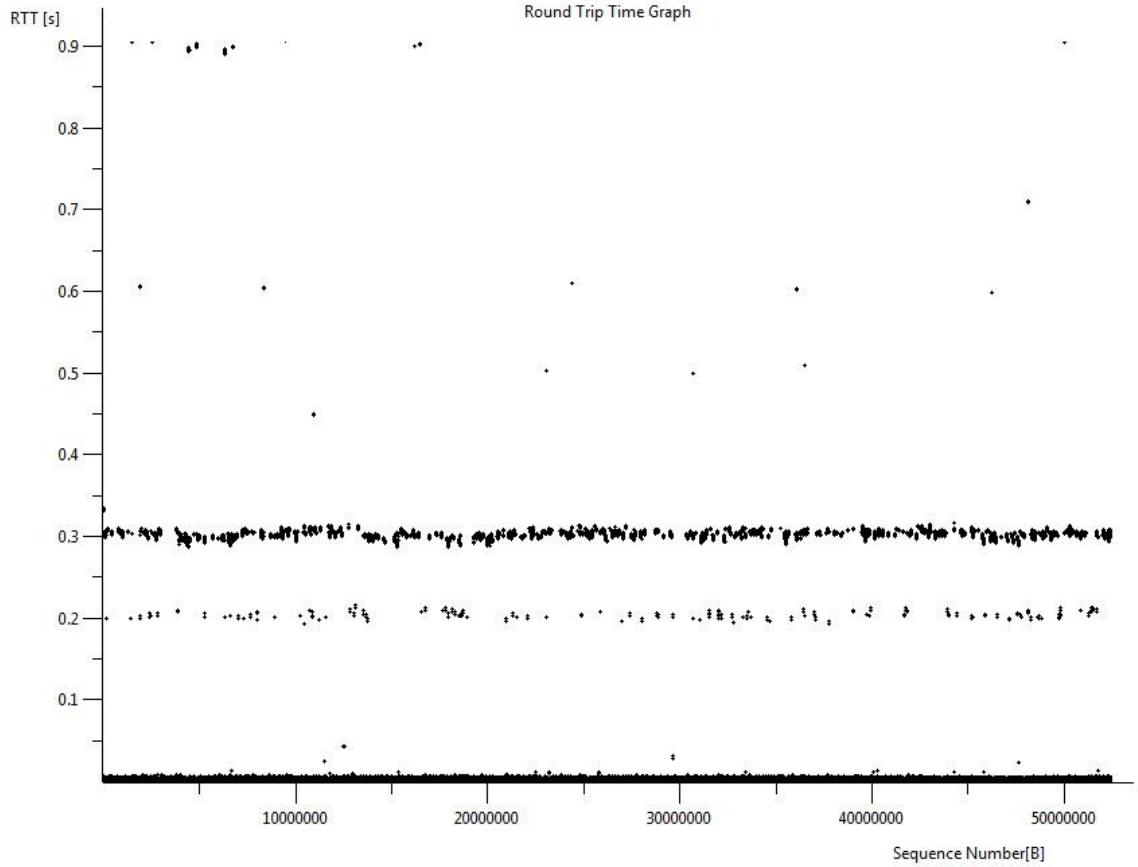
Pri nastavení filtra na tcp.analysis.ack_lost_segment sa zobrazia stratené pakety. Pri celom pokusnom meraní bolo stratených 14 paketov. Čo je stratovosť z celkového počtu paketov 303167 je 0,004%. Stratovosť len z paketov obsahujúce TCP teda 193232 paketov je chybovosť 0,007%.

8.3.4 Round Trip Time (RTT)

Grafy RTT pre TCPje možné získať pri nastavení filtra pre TCP spojenie. Vo filtri nastavíme hodnotu tcp. Po vybraní paketu z toku, o ktorý je záujem sa v menu vyberie nasledovne: Statistics → TCP Stream Graph → Round Trip Time Graph



Graf č.3 RTT pre FTP prenos z adresy 192.168.1.100 na 192.168.1.67

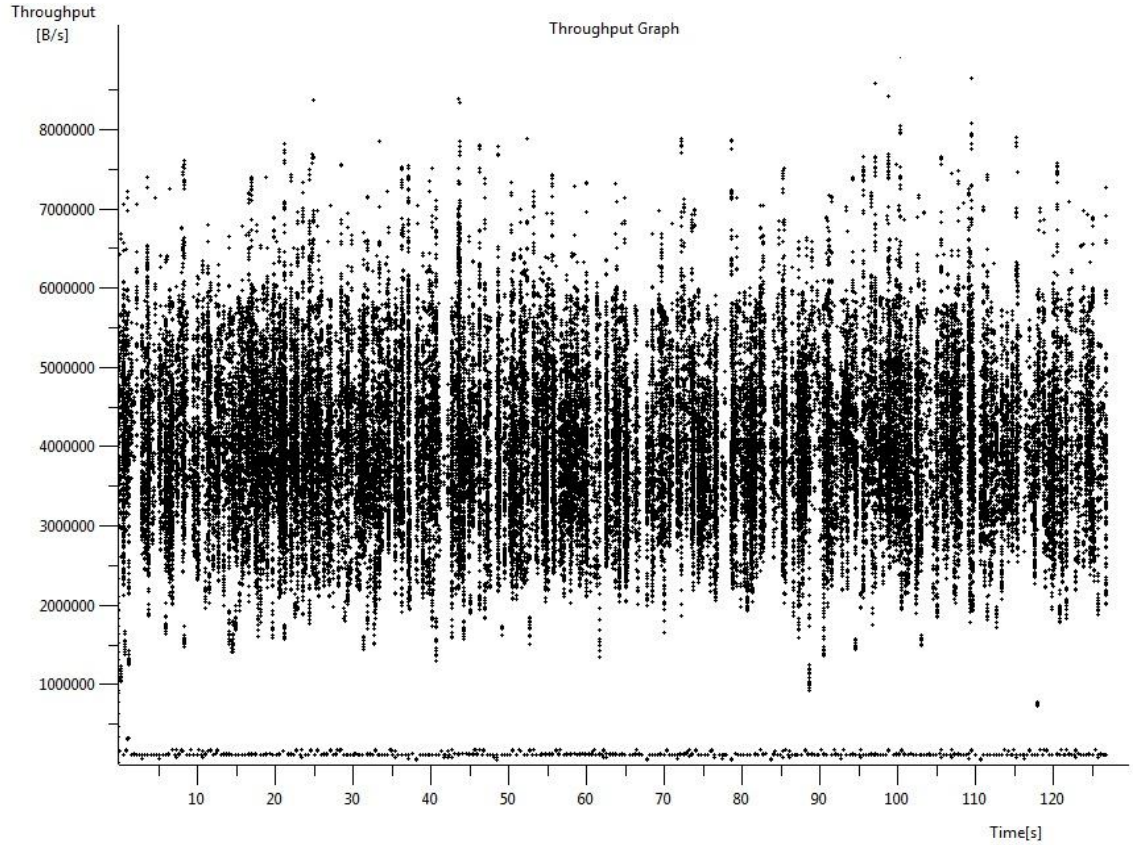


Graf č.4 RTT pre FTP prenos z adresy 192.168.1.100 na 192.168.1.12

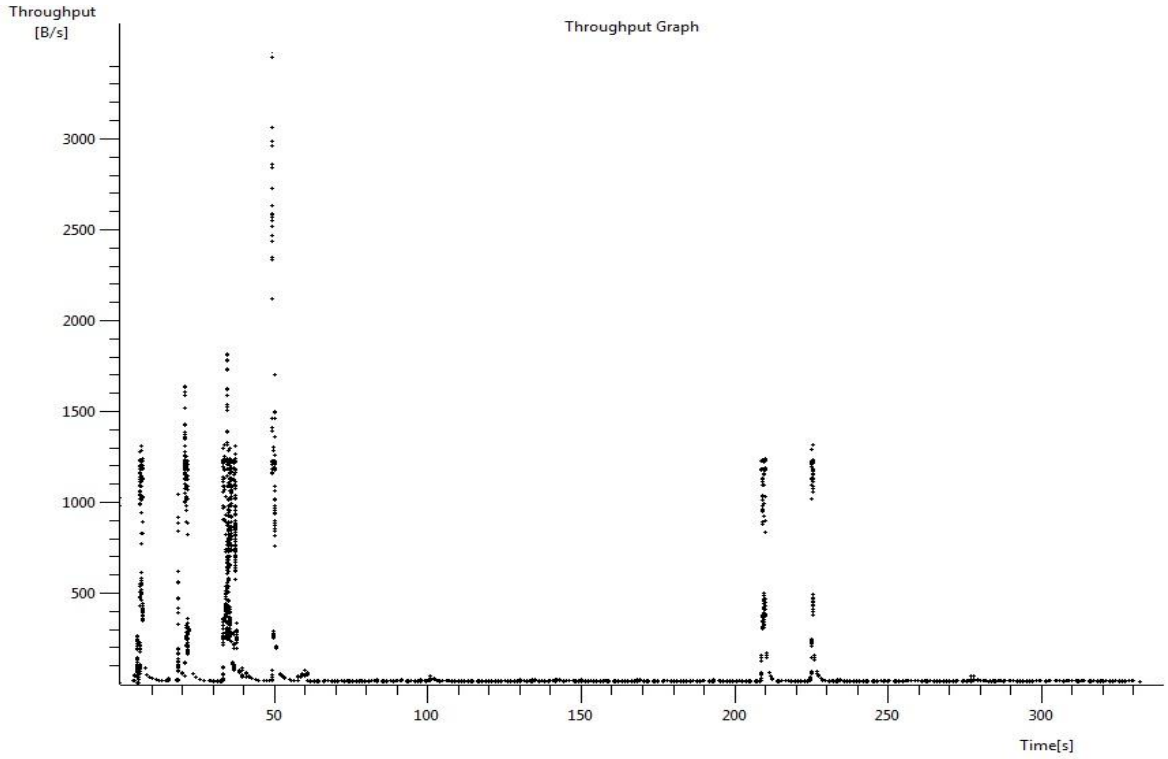
Z grafov je vidno, že hodnoty RTT (Round Trip Time) pre FTP prenos sú u oboch prenosov takmer totožné. Maximálna hodnota RTT je 0,3s. Segmenty s vyššou hodnotou RTT vzhľadom na ich malý počet môžeme zanedbať.

8.3.5 Priepustnosť pri TCP komunikácii

Podobne ako pri RTT si vyberieme požadovaný paket daného toku a v menu sa vyberie: Statistics → TCP Stream Graph → Troughtput Graph



Graf č.5 priepustnosť pri FTP prenose z adresy 192.168.1.100 na 192.168.1.67

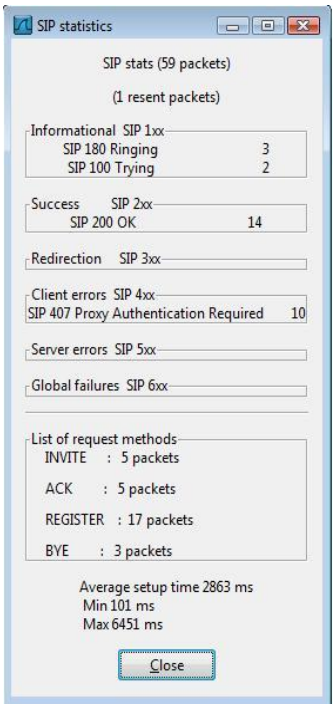


Graf č.6 priepustnosť pri VNC komunikácii medzi adresami 192.168.1.67 a 192.168.1.10

Ako je vidno z grafov priepustnosti tak pri FTP prenose sa priepustnosť držala v rozmedzí hodnôt 2MB/s – 6MB/s tak pri VNC prenose táto priepustnosť narastala len čase mojej aktívnej práce so vzdialenou správou.

8.3.6 Analyzovanie VOIP

Pre zistenie počtu paketov s protokolom SIP, ktoré prechádzali sieťou stačí v menu vybrať: Telephony → SIP



Obr. 21 SIP štatistiky

Ako je vidno z obrázka celkovo riadiacich paketov s protokolom bolo 59. Pre potvrdenie je možné zadať do filtra „sip“ a wireshark vyfiltruje týchto 59 paketov.
Pri výbere v menu Telephony → RTP → Show All Streams sa zobrazí tabuľka so všetkými spojeniami.

Detected 12 RTP streams. Choose one for forward and reverse direction for analysis

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.1.10	40046	192.168.1.67	40044	0x26E9	g711A	140	0 (0,0%)	23,95	2,94	2,82
192.168.1.10	40048	192.168.1.12	40014	0x2EA6	g711A	11623	0 (0,0%)	26,35	3,24	2,85
192.168.1.11	40024	192.168.1.67	40046	0x440D	g711A	10626	0 (0,0%)	38,47	4,73	2,92
192.168.1.12	40014	192.168.1.10	40048	0x7E87	g711A	11586	27 (0,2%)	163,90	13,27	0,48
192.168.1.67	40044	192.168.1.10	40046	0x5D03	g711A	148	1 (0,7%)	41,00	2,87	2,82
192.168.1.67	40046	192.168.1.11	40024	0x4509	g711A	10548	68 (0,6%)	47,90	7,93	2,86
192.168.1.10	40004	192.168.1.67	40046	0xFEFFFFFF	h263	227	0 (0,0%)	34,00	32,74	0,83
192.168.1.10	40010	192.168.1.12	40012	0xFEFFFFFF	h263	7939	0 (0,0%)	34,88	32,92	1,98
192.168.1.11	40022	192.168.1.67	40004	0xFEFFFFFF	h263	7410	0 (0,0%)	39,86	33,45	1,99
192.168.1.12	40012	192.168.1.10	40010	0xFEFFFFFF	h263	8123	11 (0,1%)	69,68	36,13	2,07
192.168.1.67	40046	192.168.1.10	40004	0xFEFFFFFF	h263	106	0 (0,0%)	34,90	32,38	0,50
192.168.1.67	40004	192.168.1.11	40022	0xFEFFFFFF	h263	7210	22 (0,3%)	36,79	35,28	1,98

Tabuľka č.10 zoznam VoIP spojení

Ako je vidno z tabuľky č. 10 počas zaznamenávania paketov boli vytvorené tri spojenia. Ku každému spojeniu sú zobrazené údaje ako počet stratených paketov, jitter typ použitého kodeku, počet prenesených paketov atď. Najväčší jitter malo spojenie Stanica_4 → Stanica_3 aj keď priemernú hodnotu malo najnižšiu. Dôvod vzniku týchto hodnôt je pripísane tomu, že zdroj hlasu bol využitý MP3 prehrávač, ktorý mal nastavenú vysokú hlasitosť. U ostatných VoIP hovorov priemerná hodnota jitteru sa pohybovala okolo 2,8ms.

Program Wireshark umožňuje podrobnejšie analyzovať jednotlivé hovory s tým že dokáže dekódovať jednotlivú komunikáciu do audio súboru pod podmienkou, že komunikácia nebola šifrovaná.

8.3.7 Analyzovanie video streamu

Pre vyfiltrovanie UDP video streamu treba zadať ako filter: (ip.addr eq 192.168.1.100 and ip.addr eq 192.168.1.255) and (udp.port eq 54137 and udp.port eq 1234). V menu Statistics → Summary. Z okna, ktoré sa otvorilo je možné zistiť:
Priemerná rýchlosť: 127,631kB/s
Veľkosť prenesených dát: 45,72MB
Priemerná veľkosť paketu: 1358B

Tak ako aj u VoIP komunikácie tak pri analýze UDP toku je možné rekonštruovať video stream. Je nutné kliknúť na jeden paket v toku pravým tlačidlom myši. V menu je nutné vybrať Follow UDP Stream. V ďalšom okne zvoliť typ dát RAW a uložiť v tomto prípade súbor s koncovkou „.ts“.

9 Záver

Cieľom tejto práce bolo oboznámenia čitateľa s parametrami dátových sietí ich vlastnosťami a ako vplývajú tieto vlastnosti na služby, ktoré sú poskytované cez dátové siete. V prvej časti práce boli dátové siete rozdelené na dva typy. Siete používajúce prenosové médium vzduch a siete používajúce ako médium iný materiál (optický alebo metalický spoj). Tu boli vymenované ich vlastnosti a ako ovplyvňujú služby, ktoré využívajú tieto médiá na prenos. Ďalšia časť práce sa venuje protokolovej sade TCP/IP a ich vlastnosťami. Boli vymenované niektoré protokoly, ktoré sa využívajú na prenos dát a ich vplyv na parametre týchto prenášaných dát ako sú rýchlosť alebo chybovosť. V ďalšej časti sa práca venovala službám, ktoré užívatelia dátových sietí využívajú. Boli vymenované nároky týchto služieb a metódy ako dosiahnuť optimálne parametre pre jednotlivé služby. V záverečnej časti teoretickej pasáže boli vymenované metódy merania parametrov dátových sietí a ich vlastnosti.

Praktická časť práce sa venovala analyzovaniu dátovej prevádzky pomocou programu Wireshark. V navrhnutej dátovej sieti sa analyzoval sa celkový tok veľkosť prenesených dát priemerná rýchlosť. Potom sa analyzovali jednotlivé dátové toky, ktoré boli rozdelené podľa služby a to prenos VoIP, prenos videa, a prenos dátových súborov. Analyzovalo sa zastúpenie týchto služieb v celkovom toku ako aj jednotlivá analýza parametrov služieb ako priemerná prenosová rýchlosť, veľkosť prenesených dát, priepustnosť, jitter.

V ďalšom smerovaní práce je možnosť využiť na analýzu parametrov inú metódu a vzájomne porovnať dosiahnuté výsledky a navrhnúť optimálne nastavenia jednotlivých metód pri spoločnej analýze dátových sietí.

10 Použitá literatúra

[1] SZIGETI, T., HATTINGH, CH. End-to-End QoS Network Design. Cisco Press, ISBN 1-58705-176-1, USA, 2004
[2] BEURAN, R., IVANOVICI, M., DOBINSON, B. Network Quality of Service Measurement System for Application Requirements Evaluation. Proceedings of the 2003 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2003), July 20-24, 2003, Montreal, Canada, ISBN: 1-56555-269-5, pp.380-387, 2003
[3] JEŘÁBEK JAN. Pokročilé komunikační techniky. FEKT VUT, Apríl 16, 2010, Brno, Česká republika
[4] ŠKORPIL VLADISLAV, Služby telekomunikačních sítí. FEKT VUT, Apríl 17, 2009, Brno, Česká republika
[5] PROKOPEC JAN, HANUS STANISLAV, Systémy mobilních komunikací. FEKT VUT
[6] TOMÁŠ GIERTLI, Hodnotenie kvality služieb v systémoch prenosu údajov. 2006 http://www.qos-diplomka.webzdarma.cz/index.htm
[7] JAROMÍR TŘÍSKA, Technológie počítačových sietí, SPŠE Piešťany 2003 http://www.spsepn.edu.sk/skola/pk_info/studium/ucebtext/ele/siete/prot_arch.pdf
[8] LUVR s.r.o., Mobilní datové sítě, http://www.radiostanice-vysilacky.cz/radiostanice/radiostanice-motorola/radiomodemy/mobilni-datove-site/
[9] ZBONČÁK JOZEF, Kvalita služby QoS a kvalita vnímania QoE, http://www.posterus.sk/?p=11948
[10] http://networkninja.co.za/cisco-systems/wlan-standards/
[11] http://pc-site.owebu.cz/?page=PTCP
[12] wiki2.cnl.sk/pub/Sandbox/ZoznamPrac/dp.doc
[13] JARED SMITH, JIM VAN MEGGELEN, Asterisk : The Future of Telephony, ISBN 13: 9780596510480
[14]http://pages.cpsc.ucalgary.ca/~carey/papers/2001/measurements.pdf
[15]Cisco magement fundaments
[16]http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/
[17]http://sk.wikipedia.org/wiki/Simple_Network_Management_Protocol
[18] CHRIS SANDERS, Analýza sítí a řešení problémú programu Wireshark, Computer press, Brno2012, ISBN 978-80-251-3718-5

11 Prílohy

11.1 Postup vytvorenia video streamu v programe VLC media player

Konfigurácia na stanici so serverom:

1. V záložke *Médium* vyberieme položku *Streamovanie.*
2. V záložke súbor pridáme požadované videá určené na prehrávanie a klikneme na tlačidlo *Stream.*
3. V ďalšom okne nazvanom Výstup streamu a podmenu *Zdroj* klikneme na tlačidlo *Ďalej*.
4. V podmenu Ciele vyberieme metódu streamovania UDP(legacy) a klikneme *Pridať*
5. V menu nastavenia UDP zadáme všesmerovú adresu siete v ktorej sa nachádzame a chceme prevádzkovať streamované video.
6. Nastavíme nami vybraný kodek (v rámci diplomovej práce som vybral).
7. Stlačíme tlačidlo *Stream.*

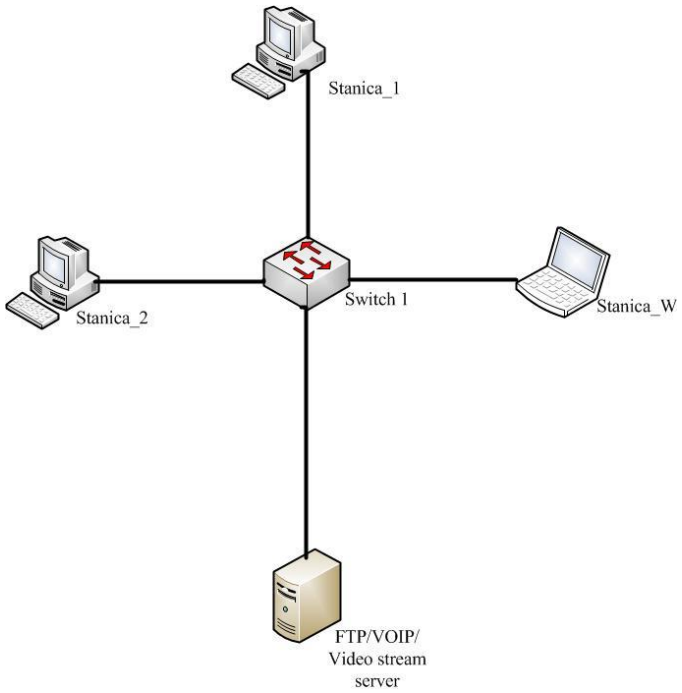
VLC media player ponúka viacero možností nastavenia streamovania, ale pre demonštráciu v sieťovej komunikácii stačí toto základné nastavenie.

11.2 Laboratórna úloha

Cieľ: Meranie parametrov siete pomocou programu Wireshark

Postup práce

1. Priraďte staniciam IP adresy a otestujte konektivitu.
2. Nastavte prepínači zrkadlenie portov.
3. Na stanici označenej ako server uveďte do prevádzky FTP server, VOIP ústredňu a streamovanie videa.
4. Na stanici s programom Wireshark spustite Wireshark.
5. Uskutočnite telefónny hovor, na jednej stanici spustite sťahovanie súboru cez FTP server a spustite streamovanie videa na druhej stanici.
6. Po ukončení sťahovania súboru z FTP serveru postupne ukončite VoIP hovor a streamovanie videa.
7. Z TCP spojenia zistite priepustnosť, RTT, rýchlosť prenosu, stratovosť a graficky znázornite veľkosť TCP z celkovej prevádzky.
8. Z VoIP komunikácie zistite jitter, počet stratených paketov a typ použitého kodeku.
9. Zistite priemernú rýchlosť, veľkosť prenesených dát a priemernú veľkosť paketu pri video streame.



Návod:

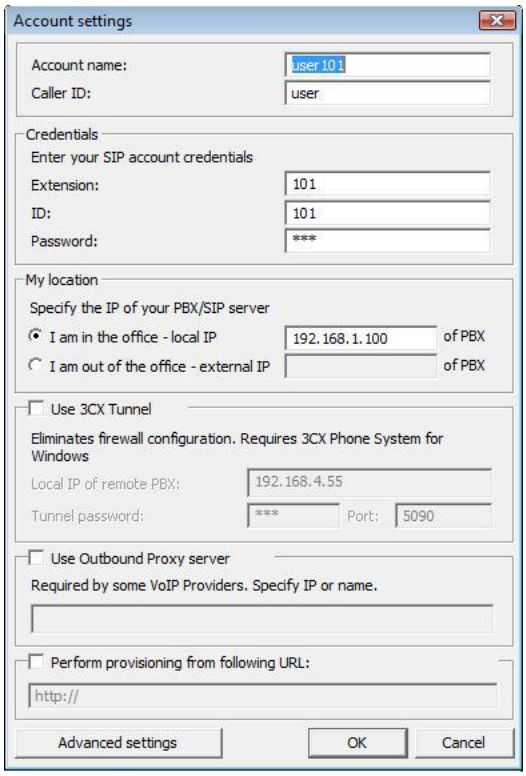
1. Staniciam priraďte IP adresy podľa tabuľky

Názov stanice	IP adresa
server	192.168.1.100
Stanica_1	192.168.1.11
Stanica_2	192.168.1.12
Stanica_W	192.168.1.13
Switch_1	192.168.1.1

Tabuľka č.1

Pomocou príkazu pinč otestujte pripojenie

2. Do webového prehliadača zadajte IP adresu prepínača. Prístupové údaje sú: meno:admin heslo: 1234. V prejdite na zrkadlenie portov a nastavte zrkadlenie na príslušný port kde je pripojená stanica s názvom Stanica_W.
3. Na stanici Server spustite FTP server GuildFTPd (ikona spustenia je na ploche). Vytvorte účet. Meno: user heslo:user. Hodnotu maximálnej rýchlosti sťahovania nastavte na 1000kB/s.
   V menu ponuke štart nájdite 3CX Phone System a spustite Managment Console. Prístupové údaje sú: meno:admin heslo: admin. Nastavte IP adresu servera na 192.168.1.100 a vytvorte užívateľské kontá (extentions) 101 a 102.
   Pre nastavenie streamovaného videa postupujte v návode uvedenom v prílohe.
   Na staniciach Stanica_1 a Stanica_2 spustite 3CX Phone a zaregistrujte užívateľské kontá 101 (Stanica_1) a 102 (Stanica_2). V hlavnom menu vyberieme accounts a pridáme nového užívateľa viď. obrázok 2.



Obrázok č.2

4. Pustite Wireshark. Capture → Interfaces → Start. Vyberieme požadovanú sieťovú kartu
5. Uskutočníme hovor. Pomocou programu Total Commander sa pripojte na FTP server. Net → New FTP Connection... Treba odkliknúť políčko anonymous connction. Zadajte IP adresu FTP servera. Zadajte meno a heslo a vyberte súbor začnite sťahovať.
6. Po stiahnutí súboru potupne ukončite VoIP a streamovnie videa a uložte v programe Wireshark zachytené pakety.
7. Pomocou filtra TCP odfiltrujeme pakety. V menu Statistics → TCP Stream Graph zobrazte postupne požadované grafy. V Menu Statistics → Conversation list → TCP(IPv4 & IPv6) zobrazte tabuľku a vyhľadajte požadované informácie o rýchlosti a veľkosti prenesených dát. Záložka IO Graph zobrazí celkovú prevádzku po doplnená filtrov hodnotami *tcp udp trp* zobrazíte jednotlivé toky. Filter tcp.analysis.ack_lost_segment zobrazí počet stratených paketov.
8. Menu Telephony → RTP → Show All Streams zobrazí požadované informácie v prehľadnej tabuľke.
9. Z dostupných informácií odfiltrujte udp video stream a v menu summary odčítajte hodnoty.

Zoznam použitých prístrojov a programov

1x Aktívny prepínač Zyxel GS 1510
4x PC
VLC media player
3CX Phone System
3CX Phone
GuildFTPd
Wiresark

11.3 Zoznam skratiek

ATM – Asynchronous Transfer Mode
ARP – Address Resolution Protocol
BSC – Base Station Controler
BSS – Base Station Subsystem
BTS – Base Transciever Station
CAL – Core Agent Logic
CDMA – Code division multiple access
CLI – Command Line Interface
CRC – Cyclic Redundancy Check
CSMA-CA – Carrier Sense Multiple Access with Collision Avoidance
DHCP – Dynamic Host Configuration Protocol
DifServ – Differentiated Services
DSSS – Direct-Sequence Spread Spectrum
EDGE – Enhanced Data rates for GSM Evolution
FCS – Frame check Sequence
FDD – Frequency Division Duplex
FHSS – Frequency-hopping spread spectrum
FTP – File Transfer Protocol
GPRS – General Packet Radio Service
GSM – Global System for Mobile communication
HSCSD – High Speed Circuit Switched Data
HTTP – Hypertext Transport Protocol
ICMP – Internet Control Massage Protocol
IntServ – Intagrated Services
IMAP –Internet Message Access Protocol
IPv4 – Internet Protocol version 4
ISDN – Integrated Services Data Network
LAN – Local Area Network
MAC –Media Access Control
MIB – Management Information Base
MN – Network Management
MOS – Mean opinion score
NSS –Network and Switching Subsystem
QoE – Quality of Experience
QoS – Quality of Service
OFDM – Orthogonal frequency-division multiplexing
PDU – Protocol Data Unit
RTP – Real-Time Transport Protocol
RTCP – RTP Control Protocol
SCTP – Stream Control Transmission Protocol
SIP – Session Initiation Protocol

SNMP – Simple Network Management Protocol
TCP – Transmission Control Protocol
TCP/IP – Transmission Control Protocol / Internet Protocol
TOS – Tipe Of Service
TTL – Time To Live
UDP – User Datagram Protocol
VoIP – Voice over IP
WAN – Wide Area Network
Wimax – World Interoprability For Microwave Access